International Civil Aviation Organization

A41-WP/281[1]
EX/121
28/7/22

WORKING PAPER

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

CYBERSECURITY GOVERNANCE IN CIVIL AVIATION

(Presented by Oman)

EXECUTIVE SUMMARY

This paper discusses the importance of effective governance in ensuring the protection of civil aviation against cyber-attacks, highlighting it as a fundamental factor in strengthening coordination and communication processes to safeguard civil aviation against cyber-attacks.

Cyber-attacks are best countered by effectively implementing cybersecurity requirements. The first step in this process would be for the Civil Aviation Authority (CAA), responsible for regulating the industry, to establish a clear structure. This structure should include the primary function of regulation (legislation and oversight) and other functions to be assigned to various stakeholders.

Action: The Assembly is invited to endorse the following recommendations:

a) urge States, through their civil aviation authorities, to establish and adopt a standardized civil aviation cybersecurity governance structure to ensure a harmonized and proper incorporation of international obligations into their national regulatory frameworks, which supports the safety and security of civil aviation against cyber-attacks;
b) urge States to develop, maintain and coordinate the implementation of aviation cybersecurity requirements by the appropriate civil aviation authority entity responsible for implementing the requirements of Annex 17 to the Chicago Convention; and
c) provide support, assistance and guidance to States to develop a standardized aviation cybersecurity governance structure.

Strategic Objectives:	This working paper relates to the Strategic Objective: *Security and Facilitation.*
Financial implications:	The action items referred to in this paper are expected to be undertaken based on the availability of financial and human resources within Contracting States. Such action items can also be integrated in the Global Aviation Security Plan (GASeP).
References:	*Aviation Cybersecurity Strategy* Annex 17 – *Aviation Security* Universal Security Audit Programme - Continuous Monitoring Approach (USAP-CMA) Doc 8973, ICAO *Aviation Security Manual*

[1] Arabic version provided by Oman.

1. INTRODUCTION

1.1 This paper aims to achieve ICAO's *No Country Left Behind initiative* by implementing Standard 2.1.2 of Annex 17 – *Aviation Security*: "Each Contracting State shall establish an organization and develop and implement regulations, practices and procedures to safeguard civil aviation against acts of unlawful interference taking into account the safety, regularity and efficiency of flights."

1.2 National legislation developed based on best practices and in compliance with the 1944 Chicago Convention and cybersecurity-related Standards and Recommended Practices (SARPs) in Annex 17, as well as the 2010 Beijing Convention and Protocol, provide the most critical provisions regulating the industry and determine how tasks and responsibilities are assigned to personnel to safeguard civil aviation against acts of unlawful interference.

1.3 The international obligation to enhance civil aviation security and facilitation by way of introducing requirements at the national level should follow a clear and structured plan, thereby ensuring the establishment of comprehensive national legislation that would help operational staff mitigate risks and threats and safeguard all civil aviation facilities from acts of unlawful interference.

1.4 Developing cybersecurity regulations and procedures in compliance with Annex 17 requirements and security-related provisions in other Annexes to the Chicago Convention is of paramount importance, as many regulatory and functional aspects must be taken into consideration according to the work environment established by CAAs through national legislation. The objective is to ensure that said regulations and procedures are implemented in line with the international obligation to enhance civil aviation security and safeguard the sector against cyber-attacks.

2. INTERDEPENDENCE OF THE AVIATION NETWORKS

2.1 The civil aviation information network is connected to many stakeholders, including security service providers, air navigation facilities, ground services providers, air cargo, catering, and other relevant operational and governmental entities. Networks are also internationally interlinked on the operational level by sending and receiving relevant information.

2.2 The civil aviation industry is increasingly relying on technology in all aspects of its operations. Driven by the need to safeguard the industry against cyber-attacks, which may pose a serious risk to this vital industry, CAAs carry out the regulatory functions of legislation and oversight in this field to ensure that activities are aligned with ICAO policies and methodologies. To this end, they must be able to attract resources with the necessary expertise and competencies to develop cybersecurity legislation and properly undertake the role of oversight.

2.3 The civil aviation industry is increasingly dependent on the availability of information, communication and surveillance systems, as well as data integrity and confidentiality. Therefore, CAAs need to accelerate the development of legislation and establish an oversight system that requires industry stakeholders to safeguard their systems by developing and implementing mitigation measures. That can only be achieved through proper coordination and division of cybersecurity tasks and responsibilities. Notably, Annex 17 provides for an international obligation to enhance cybersecurity by the appropriate aviation security entity in the CAA.

3. CYBERSECURITY GOVERNANCE

3.1 It is vital to have a clear understanding of the roles and responsibilities related to cybersecurity from a regulatory and oversight perspective. The objective is to establish an efficient and sustainable operational framework to avoid any overlap in functions and responsibilities between entities concerned with aviation cybersecurity and to comply with all requirements to safeguard the sector against acts of unlawful interference. This matter has become of significant importance, particularly as cyber-attacks constitute an emerging threat and a significant concern to the international aviation security community.

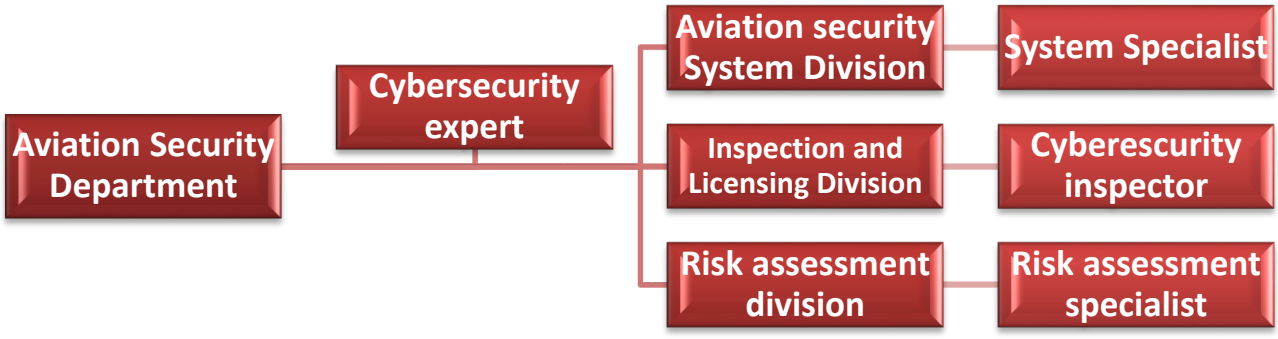
3.2 CAAs must pay due attention to the security of civil aviation by addressing the different concerns to ensure a secure, safe, regulated, economical and environmentally friendly aviation sector. This is best achieved by developing a comprehensive regulatory governance mechanism and establishing operational enablers that protect against cyber-attacks with the latest technologies and communication systems.

3.3 The importance of such a framework is now more significant with the need to address the growing pace of cyber threats and attacks worldwide and to cope with their high complexity and varying motives, such as organized crime, financial or political goals, etc., as more businesses and institutions switch to the digital domain through widespread digitalization, e-services and integration among institutions around the world, including among civil aviation entities.

4. CYBERSECURITY GOVERNANCE WITHIN A CIVIL AVIATION AUTHORITY (NATIONAL LEVEL)

4.1 Regulating cybersecurity is a responsibility assigned to the appropriate civil aviation security entity responsible for establishing and maintaining cybersecurity systems. The licensing and oversight section implements the various quality assurance activities. Also, the risk assessment section is responsible for assessing cyber-security risks[2].

4.2 The different industry bodies carry out day-to-day operations in compliance with regulatory cybersecurity requirements.



[2] Example of a CAA Aviation Security Entity structure

5. OPERATIONAL LEVEL

5.1 Operational entities must comply with national requirements, set standard operating procedures and implement necessary measures to protect critical civil aviation information and communications technology systems and data.

— END —