International Civil Aviation Organization

Tenth Meeting of the Air Traffic Management Sub-Group (ATM/SG/10) of APANPIRG

Video Teleconference, 17 – 21 October 2022

Agenda Item 8: Any other business

AIR TRAFFIC MANAGEMENT SECURITY AND CYBERSECURITY

(Presented by the Secretariat)

SUMMARY

This paper presents information on ICAO security requirements relating to Air Traffic Services Providers (ATS Providers) and Air Traffic Management. The paper also presents a review of activities related to aviation cybersecurity, including those mandated by the Assembly.

1. INTRODUCTION

1.1 Aviation security SARPs are contained in Annex 17 - *Security* and have relevance to many other Annexes including, but not limited to, Annex 2, 6, 8, 9, 10, 11, 14 and 18. There are also connections with PANS Docs 4444 and 8168.

1.2 Annex 17 – *Security* requires States to develop and implement a National Civil Aviation Security Programme (NCASP), which should specify the roles and responsibilities of all the organizations and agencies, including Air Traffic Services (ATS) Providers that may be involved in security operations. The NCASP addresses the whole range of security activities including, *inter alia*, threat and risk assessment, staff selection and training (in security-related matters), access control and other preventive security measures, management of response to acts of unlawful interference, and quality control.

1.3 Not all provisions of the NCASP will be applicable to the ATS Providers. The NCASP identifies the specific responsibilities of each of the parties that have a role in security operations.

2. DISCUSSION

Aviation Security Aspects Relating to ATM

2.1 There are a number of Standards and Recommended Practices (SARPs) with particular relevance to ATS Providers and ATM security contained in Annex 17 – *Security*. These requirements are found in sub-chapter 3.5 (Air traffic service providers) and in sub-chapter 5.2 (Response); whereas cybersecurity provisions are in sub-chapter 4.9 (Measures relating to cyber threats).

2.2 States' compliance with the above mentioned Standards are subject to auditing under the ICAO Universal Security Audit Programme - Continuous Monitoring Approach (USAP-CMA).

2.3 In accordance with its leadership role, and in recognition of the vital role played by ATS Providers and the security of ATM, ICAO has drafted guidance to assist States to establish and implement the appropriate security provisions as required by the relevant SARPs, which would include the physical and electronic protection of all relevant facilities and equipment. The Air Traffic Management Security Manual (Doc 9985) is available to States for convenience. This Manual complements the *Aviation Security Manual* (Doc 8973 – Restricted) and provides guidance on security issues specific to ATM in order to assist States and ATS Providers in implementing appropriate security provisions to meet the published requirements of the NCASP. In addition, the manual provides guidance to the ATS Providers on provision of ATM security services in support of national security and law enforcement requirements, and guidance on protection of the ATM system infrastructure from threats and vulnerabilities.

2.4 The 12th Edition of the ICAO Aviation Security Manual (Doc 8973) includes a chapter that provides guidance on the implementation of cybersecurity provisions in Annex 17.

2.5 The 3rd Edition of the ICAO Aviation Security Global Risk Context Statement (RCS) ICAO Doc 10108 (2022) provides a methodological approach to Risk assessment (including ATM/cyber risks) – to support States in developing their national threat/risk evaluation/mitigation system. It continues to define the risk of cyber-attacks used as an act of unlawful interference against civil aviation as Low. In the 3rd Edition of the RCS, the Aviation Security Panel maintained its assessment of cyber threats against civil aviation as Medium which highlights the importance of addressing cyber threats and risks that may impact aviation safety and security.

Cybersecurity Action Plan

2.6 In line with the Assembly Resolution A40-10, ICAO developed and published in November 2020 the Cybersecurity Action Plan (CyAP) to support States and stakeholders in implementing the Aviation Cybersecurity Strategy. The CyAP provides the foundation for ICAO, States and stakeholders to work together, and proposes a series of principles, measures, and actions to achieve the objectives of the Cybersecurity Strategy's seven pillars (International cooperation; Governance; Effective legislation and regulations; Cybersecurity policy; Information sharing; Incident management and emergency planning; Capacity building, training and cybersecurity culture).

2.7 Taking into account the changing priorities of Member States due to the ongoing COVID-19 pandemic, and the experience of States and stakeholders in implementing aviation cybersecurity initiatives in their States and organizations, ICAO conducted a revision of the CyAP and published the second edition of the document in January 2022. The review included streamlining the document to be more concise and clearer and the action items were clarified in terms of actions, indicators, and initiation time.

Strengthening the Mechanism to Address Cybersecurity in ICAO

2.8 The 40th Session of the ICAO Assembly noted the multiple bodies involved in addressing cybersecurity in ICAO and expressed concern about the potential for gaps, duplication, inconsistency and loss of transparency. To address these concerns, the Assembly called on ICAO to bring the work of these groups under the aegis of an overarching structure, and discussed a set of criteria, which could underpin a revised cybersecurity governance structure.

2.9 The Council, during its 218th Session, endorsed the methodology for the development of the Feasibility Study and Gap Analysis on the Mechanism to Address Cybersecurity. The first two phases of the study were presented during the 219th Session. The Council requested the Secretariat to further consider and update the feasibility study, and delegated authority to the President of the Council to consider the establishment of a small working group composed of Council Representatives and Air Navigation Commission (ANC) Members to develop Phase 3 of the feasibility study with the assistance of the Secretariat. The Small Working Group met extensively between November 2020 and January 2021, considered several governance options and recommended a solution which was approved by the Council during its 222th Session. The new governance structure for cybersecurity in ICAO includes:

a) evolving the Secretariat Study Group on Cybersecurity to become a Cybersecurity Panel reporting to the Aviation Security Committee of the ICAO Council;

b) evolving the Trust Framework Study Group to be integrated within the ANC Panel structure; and

c) establishing an Ad-Hoc Cybersecurity Coordination Committee (AHCCC) under the Council. The Committee membership comprises one member from each of the Air Transport Committee, Aviation Security Committee, Air Navigation Commission, and every ICAO Panel and expert group addressing elements of cybersecurity in their work programme. The Committee is expected to offer the Council, and everyone involved in cybersecurity-related activities in ICAO, a single focal point for all ICAO cybersecurity-related activities, hence enhancing the accountability, transparency, efficiency, and coordination of ICAO's work on aviation cybersecurity and cyber resilience. The Council, during its 224th Session, approved the Terms of Reference of the AHCCC.

2.10 Following the Council's decision on the new governance structure, the Cybersecurity Panel was established during the 225th Session and held its first meeting in May 2022. The ANC, during its 219th Session, approved the evolution of the Trust Framework Study Group into a new ANC Panel to continue the work on the International Aviation Trust Framework.

Development of an International Aviation Trust Framework

2.11 Since its 223rd Session, the Council has discussed the development of an International Aviation Trust Framework. It will continue to progress this work, including the concept of operations and the governance of such framework.

Adequacy of international air law instruments to address cyber-attacks on civil aviation

2.12 The Aviation Cybersecurity Strategy calls for the analysis of the relevant international legal instruments, in order to identify existing or missing key legal provisions for the prevention, prosecution, and timely reaction to cyber incidents. This task was accordingly reflected in the Cybersecurity Action Plan as an action item for ICAO. As such, the SSGC established the Research Sub-Group on Legal Aspects (RSGLEG). The Sub-Group comprised of legal and cybersecurity experts to ensure that all expertise required to address its objectives are available. As agreed by the RSGLEG at its last meeting in January 2022, the Secretariat reported on the work conducted by the Sub-Group to the 38th Session of the Legal Committee which was held in March 2022.

Guidance Material

2.13 In line with the Cybersecurity Action Plan, ICAO developed guidance material to support States and stakeholders to address cybersecurity in civil aviation which includes the following (published on ICAO-NET under "Publications" and "Others"):

a) Guidance on Traffic Light Protocol (TLP), which provides States and stakeholders with guidance on using TLP in order to facilitate cybersecurity information sharing;

b) Cybersecurity Policy Guidance, which addresses the protection and resilience of international civil aviation's critical infrastructure against cyber threats, and the multilateral cooperation requirement within civil aviation as well as with external authorities. The guidance also addresses the need to designate the authority competent for aviation cybersecurity, and includes a template to support States and stakeholders to develop a Cybersecurity Policy; and

c) Cybersecurity Culture in Civil Aviation, which supports the design and implementation of a robust cybersecurity culture, building on civil aviation's success in implementing safety and security cultures.

Capacity Building

2.14 In 2020, ICAO developed a Cybersecurity Training Roadmap to support the Organization's efforts to build the capability to deliver appropriate, coherent and relevant aviation cybersecurity training to States and stakeholders. The Cybersecurity Training Roadmap supports the Aviation Cybersecurity Strategy and the Cybersecurity Action Plan. Its development also supports Assembly Resolution A40-25: *Implementing Aviation Training and Capacity Building Strategies*, which lays out how ICAO, through training activities, shall assist and support States with the development of sufficient human resources and capacity. Following the Training Roadmap, ICAO began building a cybersecurity training portfolio which includes to-date the following courses:

2.15 Foundations of Aviation Cybersecurity Leadership and Technical Management: The course was developed in partnership with Embry-Riddle Aeronautical University and began delivery in October 2021. It is a comprehensive awareness course that covers all aspects of cybersecurity addressed in the Aviation Cybersecurity Strategy.

2.16 Managing Security Risk in Air Traffic Management (ATM): The course was developed in partnership with EUROCONTROL. It covers ATM security including both physical and cybersecurity elements. The first session of the course will be delivered in November 2022.

2.17 Cybersecurity Oversight in Civil Aviation: The course is being developed in partnership with the United Kingdom's Civil Aviation Authority. It will cover key aspects that would support States in designing and implementing their oversight obligations for aviation cybersecurity.

Raising Awareness and Outreach Activities

2.18 Raising awareness of States and stakeholders to the importance of addressing cybersecurity in civil aviation has been a core activity of ICAO. The Organization continues to be heavily involved in the organization, and/or participation in, national, regional, and international conferences, meetings, and webinars in order to promote cooperation between all stakeholders in the cybersecurity and cyber resilience field, as well as promote the implementation of the Aviation Cybersecurity Strategy and the Cybersecurity Action Plan.

Audit of Cybersecurity Obligations under the (USAP-CMA)

2.19 The objective of the Universal Security Audit Programme – Continuous Monitoring Approach (USAP-CMA) is to improve global aviation security through auditing and continuous monitoring of the aviation security performance of Member States. Auditors identify the documentation in which the requirement is established for operators or entities to identify their critical information and communications technology systems and data used for civil aviation purposes. They also ensure this requirement covers the assessment, development and implementation of measures to protect such information and systems from unlawful interference. Once the requirement is identified, auditors ensure that responsibilities for cybersecurity measures are clearly allocated.

2.20 Of the 136 States audited as at 31 December 2021, documentation-related aspects of cybersecurity preparedness were audited in 54 States. The audit results from these States indicate the following:

a) fifteen per cent of States had not established a requirement for operators or entities to identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference;

b) twenty-six per cent of States had not defined the responsibilities of operators or entities with regard to cybersecurity in civil aviation; and

c) forty-one per cent of States had not developed criteria for the protection of critical information and communications technology systems and data used for civil aviation purposes from unlawful interference.

2.21 hese results are not necessarily indicative of the global picture in relation to safeguarding aviation against cyber threats, as some States were audited remotely due to the pandemic and their results are incomplete. Moreover, the overall sample size is not representative enough to provide a high degree of confidence. However, these results clearly show that the civil aviation sector needs to enhance its efforts to address cyber threats to a baseline that allows for a consistent and harmonized protection against, mitigation of, and response to, cyber threats to civil aviation.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper; and

b) discuss any relevant matters as appropriate.

……