International Civil Aviation Organization

The Ninth Meeting of the APANPIRG ATM Sub-Group (ATM/SG/9)

Video Teleconference, 01 – 05 November 2021

Agenda Item 9: 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, additional information relating to the establishment and dissemination of the 1st Edition of the ICAO Cyber Security Action Plan (CyAP), and ongoing developments in related guidance material and resources.

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. 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 2nd Edition of the ICAO Aviation Security Global Risk Context Statement (RCS) ICAO Doc 10108 (2019) 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 December 2021 the Aviation Security Panel amended its assessment of cyber threats against civil aviation from Low to Medium which highlights the importance of addressing cyber threats and risks that may impact aviation safety and security. The updated evaluation will be included in the upcoming edition of Doc 10108.

ICAO Cybersecurity Initiatives and Projects

Cybersecurity Action Plan (CyAP)

2.6 The 1st Edition of the ICAO Cybersecurity Action Plan (CyAP) has been disseminated by ICAO State Letter ICAO State Letter AS8/1.9.1-20/114 - dated 5 November 2020.

2.7 The CyAP is a living document that 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 ICAO's Aviation Cybersecurity Strategy's seven pillars namely:

Pillar 1 - Achieve International Cooperation

Pillar 2 - Develop Governance and Accountability

Pillar 3 - Develop Effective Legislation and Regulations

Pillar 4 - Develop a Cybersecurity Policy

Pillar 5 - Develop Information Sharing Capabilities

Pillar 6 - Develop Incident Management and Emergency Planning

Pillar 7 - Develop Capacity Building, Training, and Cybersecurity Culture

2.8 The Seven Pillars of the Aviation Cybersecurity Strategy are developed in the CyAP into 29 Priority Actions, which are further broken down into 54 Tasks to be implemented by ICAO, States, and Stakeholders.

ICAO's Work on Cybersecurity and Cyber Resilience

2.9 Cybersecurity is currently managed in ICAO by the Secretariat Study Group on Cybersecurity (SSGC).

2.10 The work of the SSGC includes several areas: Review of the International Air Law framework to ensure that cyber-attacks against civil aviation can be prosecuted, development of guidance material on areas identified in the CyAP, monitoring the implementation of the Aviation Cybersecurity Strategy, identification of possible cyber-attack scenarios, and the revision of the CyAP in order for the document to remain current and in line with Member States' priorities.

2.11 In that regards, the SSGC approved in May 2021 the publication of the first ICAO cybersecurity guidance material, "The use of Traffic Light Protocol (TLP) in Civil Aviation" which was published on 15 September 2021 via electronic bulletin EB 2021/30. The SSGC is currently working on additional guidance material to support States and stakeholders in addressing cybersecurity and cyber resilience in civil aviation.

2.12 In addition to the work of the SSGC, ICAO also has a Study Group more focused on the air navigation domain (the Trust Framework Study Group – TFSG). The groups is working on developing the foundation for an International Aviation Trust Framework to support the secure global exchange of digital information, and on the procedures, technical requirements, and guidance material supporting current and future global network requirements.

Cybersecurity Training

2.13 ICAO continues to work on capacity building initiatives in order to support States with the effective development of human resources and capabilities to manage cybersecurity and cyber resilience in civil aviation. In that regards, ICAO finalized during the past period the revision of two training courses.

2.14 The first course, "Foundations of Aviation Cybersecurity Leadership and Technical Management" is a pure cybersecurity and cyber resilience course developed in partnership with Embry-Riddle Aeronautical University including two learning tracks: a Leadership track that acknowledges and emphasizes that cybersecurity and cyber resilience is a top-down approach in any organization, and a technical management track for staff who have responsibilities in managing civil aviation cybersecurity and cyber resilience activities. This first session was held virtually in early October with additional sessions to roll-out in due course.

2.15 The second course, "Managing Security Risk in ATM", is a security-focused course that combines both classical ATM security as well as cybersecurity. The course is developed in partnership with EUROCONTROL.

Summary

2.16 States and Air Navigation Service Providers are encouraged to:

a) make use of the relevant available guidance material and resources;

b) ensure regulatory compliance with the International and National requirements for ATS Providers and ATM Security; and

c) develop, establish and implement national cybersecurity plans in line with the ICAO Aviation Cybersecurity Strategy and the Cybersecurity Action Plan..

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.