International Civil Aviation Organization

Twenty Sixth Meeting of the Communications/ Navigation and Surveillance Sub-group (CNS SG/26) of APANPIRG

Video Tele-Conference, 5 – 9 September 2022

Agenda Item 12: Cybersecurity of CNS/ATM systems

12.2 Other Cybersecurity related issues

ENSURING CYBER RESILIENCE FOR AIR NAVIGAITON SERVICE IN HONG KONG INTERNATIONAL AIRPORT AND ITS EXPANSION

(Presented by Hong Kong, China)

SUMMARY

This paper shares the experience of Hong Kong, China in provision of an effective cyber security management framework to ensure safe and secured air navigation service (ANS) for supporting operation of Hong Kong International Airport (HKIA) and its expansion into Three Runway System.

1. INTRODUCTION

1.1 With increasing digitization and interconnection of aviation systems employing commercial-off-the-shelf (COTS) information and communications technology (ICT), cyber security threats for aviation systems are becoming increasingly imminent. Systems serving ANS, airlines and airports etc. could be potential targets for cyber attack. Hong Kong, China fully supports the ICAO's initiative in ensuring cyber resilience in ANS and protecting the ANS critical information infrastructure (CII) against increasing cyber security threats. To this end, Hong Kong, China has established a cyber security management framework for pursing compliance with the cyber security control requirements stated in ICAO Doc 9985 ATM Security Manual.

1.2 With expansion of the HKIA into Three Runway System (3RS), new ANS systems with high digitization and interconnection have been put in place. Ensuring cyber resilience in ANS provisions while coping with the airport expansion is a challenging subject to address.

2. DISCUSSION

2.1 Hong Kong Civil Aviation Department (CAD) has established a CAD Air Navigation Services Cyber Security Committee (CACSC) to steer the implementation of cyber security control measures throughout the whole life cycle of ANS systems, with a view to managing risks of cyber security threats while maintaining confidentiality, integrity, availability and safety in provisions of ANS to the aviation stakeholders.

2.2 The CACSC, supported by subject matter experts (SMEs) of various ANS systems, conducted thorough analysis for the systems against all applicable cyber security control requirements in ICAO Doc 9985. Cyber security control measures were then developed and progressively implemented to secure compliance with ICAO requirements with a view to ensuring safe, secured and efficient ANS provisions.

2.3 For the purpose of promulgating cyber security policies and implementation guidelines to all the stakeholders concerned, Hong Kong, China has progressively developed the following cyber security documentation for ANS systems. These documents are subject to regular review in conjunction with the prevailing cyber security requirements promulgated by ICAO :-

(a) ***CAD Cyber Security Manual for Air Traffic Services (ATS) Systems and Services*** **(CCSM)** – it lays down the cyber security policies, goals and objectives as well as the actions required to achieve the stated goals and objectives, and defines the accountabilities and functions of a cyber security management framework for ANS systems.

(b) ***CAD Cyber Security Handbook for ATS Systems and Services*** **(CCSH)** – it provides guidelines and detailed requirements for implementation, management, training and maintenance of cyber security for ANS systems in meeting the control requirements stated in ICAO Doc 9985.

(c) ***CAD User Account Management Policy for ATS Systems and Services*** **(CUAMP) and** ***Account Control Framework*** **(ACF)** – it outlines a systematic and traceable process for administering user accounts applicable to authorised access to ANS systems.

(d) ***CAD Security Plan for Air Traffic Services (CSP)*** – it comprises the cyber and physical security plans for ANS systems. The interaction of physical and cyber security controls will complement each other for enhancing the overall security protection of the systems.

(e) ***CAD Project Procedures Handbook (CPPH)*** – it outlines the guidelines, procedures and processes to be followed in managing CAD's projects covering generic projects, small equipment projects, and large-scale/complex ANS systems projects. This ensures cyber security elements are included in early stage of the projects.

2.4 To ensure effectiveness of various control measures, internal assessment on the control measures are conducted regularly, including verification tests, inspections and audits. Besides, third party organizations are engaged to carry out independent assessments, which are based on relevant international standards, regulations, and industry best practices. Relevant recommendations have been timely implemented.

2.5 The Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF) is the government authority to prevent and combat technology crimes, and manage cyber security incidents for various CII sectors in Hong Kong. CAD has gone a step further and invited the CSTCB to carry out independent assessment and make recommendation on the overall design, information flow, network robustness and data integrity of ANS systems from cyber security perspective similar to other CII sectors.

2.6 The assessment methodology was based on a mixed of on-site/online meetings, discussions, documentation review, dataflow and workflow analysis by the CSTCB. Apart from systems, cyber security readiness of personnel and policies were other major areas being assessed, which aimed to unveil potential cyber security risks that might affect operation of ANS systems. After assessment, the CSTCB advised that the cyber security provisions of ANS systems were satisfactory.

2.7 In line with the CSTCB's recommendation, a communication mechanism was established for CAD to seek swift assistance/advice from the CSTCB for sharing intelligence and in the event of cyber security incidents, so as to upkeep cyber security robustness and integrity of ANS systems.

2.8 Cyber security incident drills were also regularly performed jointly by CAD and CSTCB. A joint physical and cyber security drill with scenarios of terrorists attempting to attack ANS systems was exercised in 2021 to enhance our incident response capability.

2.9 With satisfactory results achieved from a series of the above-mentioned verification tests, inspections, audits and drills, CAD has, over the years, successfully built a robust and effective cyber security framework to protect our ANS systems against cyber attack.

2.10 To cope with expansion of the HKIA into 3RS, a new ATC tower was recently implemented with new ANS systems installed with high degree in digitization and interconnection. CAD has engaged an independent assessor to carry out another round of independent assessment on cyber security of the new ANS systems and its associated network. The assessment was carried out in accordance with ICAO Doc 9985 and relevant national standards. After assessment, it is confirmed that there is no cyber security risk due to the expansion and our protective measures remain effective in safeguarding ANS systems against cyber attack.

2.11 In conclusion, it is only through collaborative efforts can we manage and address cyber security threats effectively. States/Administrations are encouraged to share their experience and make reference to the guidelines and best practices promulgated by ICAO or other international organization such as IATA, CANSO and ACI etc. in developing a robust and effective cyber security management framework that suit their needs.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) Note the efforts by Hong Kong, China in establishment of an effective cyber security management framework to ensure safe and secured ANS provisions to support operation of the HKIA and its expansion;

b) Seek support from ICAO in organizing seminars/workshops to facilitate sharing of experience among States/Administrations and industry partners; and

c) Encourage States/Administrations to make collaborative efforts to effectively address cyber security threats.

– – – – – – – – – – – – –