International Civil Aviation Organization

The First Meeting of Air Traffic Management Automation System Task Force of APANPIRG (ATMASTF/1)

Web-conference, 28 – 30 October 2020

Agenda Item 5: Issues and Challenges in implementation

5.9 Cyber threats and mitigation measures

A PROACTIVE AND SYSTEMATIC APPROACH IN PROTECTING DIGITISED AIR TRAFFIC SERVICES AGAINST CYBER THREATS IN HONG KONG, CHINA

(Presented by Hong Kong, China)

SUMMARY

This paper presents the proactive and systematic approach in implementation of cyber security control measures to protect the increasing digitisation of air traffic services against cyber threats in Hong Kong, China.

1. INTRODUCTION

1.1 Cyber security is an increasing challenge for aviation industry, in particular in protecting the critical infrastructure against cyber threats to Air Traffic Services (ATS). With the rapid digitisation of ATS, the Civil Aviation Department of Hong Kong, China (HKCAD) fully supports ICAO's initiative on aviation cyber security against cyber attacks that might impact the safety and security of ATS systems. With that in mind, HKCAD commits to the development and implementation of mitigation measures and controls for continuous protection of the ATS systems against cyber security threats. This information paper outlines the enhanced controls of cyber security to achieve the ultimate goal in protecting information data, physical assets or a combination thereof in HKCAD.

2. DISCUSSION

Enhanced Controls on Cyber Security in Hong Kong, China

2.1 In the world of civil aviation, a safe, efficient and sustainable transport system is a large and complex system. ATS systems are the critical components for civil aviation and composed of various air traffic control equipment which interact with each other. HKCAD has developed a cyber security management to provide a proactive and systematic approach for protecting increasing digitisation of ATS against cyber threats in HKCAD, through the establishment of Cyber Security Manual, Cyber Security Handbook and User Account Management Policy for ATS.

2.2 The above-mentioned documents, developed in accordance with relevant provisions in ICAO Annex 17 and Doc 9985, provide protection of safety-critical ATS systems against cyber threats and interference. HKCAD has identified a number of safety-critical core ATS systems and has taken

measures to put the enhanced controls on cyber security in place. Key elements of the provisions of the controls are described as below:

Cyber Security Policy

2.3 Departmental policy is part of administrative controls for HKCAD to mitigate cyber threat. HKCAD has established a cyber security steering committee with regular meetings to set up policies and steer the implementation of cyber security control measures throughout the whole life cycle of the ATS systems.

Network Infrastructure Protection for ATS systems

2.4 Interoperation among those ATS systems for information exchange is inevitable. To deal with the necessity of interoperation, proactive protection of the ATC core data network is essential for information exchange among ATS systems. ATC Data Network (ATCDN), a common Internet Protocol (IP) data network, is one of the identified safety-critical core ATS systems in HKCAD. It has been built in HKCAD's premises as the communications backbone among ATS systems. It is a high performance and resilient communication platform with a focus on the prevention of operational disruption. Networking technologies, such as virtualisation of resilient network and link aggregation using IEEE 802.3ad, are utilised to achieve high reliability of ATCDN. In addition, HKCAD established round-the-clock monitoring and reporting centre to closely monitor cyber security event in ATCDN.

2.5 The multi-tier defence-in-depth scheme for external TCP/IP unicast communication to ATS systems, comprising network equipment, firewalls, Network Intrusion Detection (NIDS) or Network Prevention System (NIPS), is devised to strengthen the protection of the network perimeter of ATCDN against cyber threats from external connections.

2.6 To further strengthen the above-mentioned scheme, data diode gateway is planned to be utilised to leverage on unidirectional communication for dissemination of surveillance multicast data from ATS systems to semi-trusted systems.

User Account Management

2.7 To protect the ATS systems from the cyber security risk of access control, HKCAD has devised a systematic and traceable process for administering user accounts applicable to authorised access to ATS systems.

System Development Life Cycle

2.8 To achieve the viability and sustainability of cyber security protection, the protection from cyber threat in mind throughout the system lifecycle of the development of ATS systems is indispensable. HKCAD has formulated its project procedures handbook, which include cyber security requirements, to safeguard against cyber threats from an early concept and design stage of a project. Besides, Independent Network Security Risk Assessment (INSA) for ATS systems is conducted in different stage of project cycle to assess the adequacy of the cyber security measures in HKCAD.

Removable Media Control

2.9 Removable media provide a common route for importing malicious content to information system. In order to mitigate the potential risk posed by the use of removable device or media in ATS operation, HKCAD has refined its workflow to strengthen the security control, such that

a removable media is scanned for malicious content by the machine prior to uploading data to ATS systems.

Software Security Patch Management

2.10 Patching vulnerabilities for critical ATS systems is key challenge to maintain the balance of security with performance. HKCAD has setup a scheme to work closely with system manufacturers to evaluate system patch when considered appropriate.

Physical Security Measures

2.11 While cyber security measures are in place for dealing with cyber threats, HKCAD also has implemented the physical security measures of ATS systems from physical threats. The physical security provision includes facility management, security guards, CCTV surveillance, access control and physical lock, etc., from perimeter security down to console/rack level.

Response to Cyber Security Incidents

2.12 The Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF) is the government authority responsible for investigation and prevention of technology crime. As the air traffic control centre of HKCAD is classified as a critical infrastructure, a direct reporting mechanism has established for HKCAD to seek swift assistance from CSTCB for handling cyber security incident. The CSTCB has been engaged to provide advice and independent assessment on cyber security measures implemented by HKCAD. Periodic drill exercises have been arranged to upkeep staff awareness and the robustness of the reporting mechanism.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;

b) encourage States to strengthen their cyber security management to protect the increasingly digitised ATS against cyber threats; and

c) discuss any relevant matters as appropriate.

– – – – – – – – – – – – –