INTERNATIONAL CIVIL AVIATION ORGANIZATION

TWENTY SEVENTH MEETING OF THE ASIA/PACIFIC AIR NAVIGATION PLANNING AND IMPLEMENTATION REGIONAL GROUP (APANPIRG/27)

Bangkok, Thailand, 5 to 8 September 2016

Agenda Item 3: **Performance Framework for Regional Air Navigation Planning and Implementation**

3.6: **Other Air Navigation Matters**

IMPLEMENTATION OF EFFECTIVE CYBER SECURITY MEASURES TO ACHIEVE A SAFE, SECURED AND EFFICIENT AIR TRAFFIC CONTROL SYSTEM IN HONG KONG, CHINA

(Presented by Hong Kong, China)

SUMMARY

This Paper shares the key elements of an effective cyber security management framework for a safe and secured ATC system as well as the latest status achieved by Hong Kong, China in pursuing the ICAO's ATM Cyber Security Manual published in 2013. Since then, Hong Kong, China has established relevant committee and Working Group to steer for proactive implementation of effective cyber security measures for the ATC system in Hong Kong. Over the past few years, a series of verification tests, inspections and audits were conducted by both internal and external experts to ascertain the effectiveness of various control measures being implemented in the ATC system concerned.

Strategic Objectives:

A: ***Safety*** *– Enhance global civil aviation safety*

B: ***Air Navigation Capacity and Efficiency****—Increase the capacity and improve the efficiency of the global aviation system*

1. INTRODUCTION

1.1 With the extensive deployment and closer interconnection of Commercial-Off-The-Shelf (COTS) Information and Communications Technology (ICT) Systems which is built on common standards rather than on the conventional proprietary equipment, Air Navigation Service Providers (ANSPs) have been facing increasing challenges to manage potential risks arising from cyber security threats. To address the growing concerns on cyber security threats, ICAO published Doc 9985 "ATM Security Manual" in 2013 setting out the principles and guidelines for protecting ATC system infrastructure.

1.2 Hong Kong, China fully supports ICAO's initiative on protecting ATC system infrastructure against the growing 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 as stated in ICAO Doc 9985.

2. DISCUSSION

2.1 In August 2013, Hong Kong Civil Aviation Department (CAD) established the CAD Air Navigation Services Cyber Security Committee (CACSC) to steer the implementation of cyber security control measures throughout the whole life cycle of ATC system, with a view to containing and mitigating risks of cyber security threats while maintaining confidentiality, integrity, availability and safety in the provision of air navigation services to the aviation stakeholders. To effectively implement cyber security policies and various control measures, the CACSC is supported by the CAD Air Navigation Services Cyber Security Working Group (CACSWG) which serves as the executive arm of the CACSC.

2.2 As a start, the CACSWG deployed the Subject Matter Experts (SMEs) of various ATC systems to conduct a thorough gap analysis for the ATC system infrastructure in Hong Kong, China against all Level 1 and Level 2 cyber security control requirements in ICAO Doc 9985 in late 2013. Based on the cost-benefit analysis, the CACSC endorsed the recommendations made by the CACSWG to implement Level 1 cyber security control requirements.

2.3 To bridge the identified gaps, a series of cyber security control measures were then developed and progressively implemented to secure the compliance with ICAO Doc 9985 Level 1 control requirements for ATC system with a view to achieving a safe, secured and efficient ATC system.

2.4 For the purpose of promulgating cyber security policies and implementation guidelines to all the stakeholders concerned, Hong Kong, China has progressively developed the following three cyber security documents since 2010 specifically for the ATC system. These documents have been revamped duly taking into account the cyber security requirements as promulgated by the ICAO Doc 9985. These three documents are :-

(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 ATC system.

(b) *CAD Cyber Security Handbook for ATS Systems and Services* (CCSH) – It provides guidelines and detailed requirements for the implementation, management, training and maintenance of cyber security for ATC system in meeting the Level 1 control requirements stated in ICAO Doc 9985.

(c) *CAD User Account Management Policy for ATS Systems and Services* (CUAMP) – It outlines a systematic and traceable process for administering user accounts applicable to authorised access to the ATC system. All officers and staff, upon satisfactory completion of proper training and competence checks, would be assessed on a need basis and granted an appropriate level of access right of the ATC system to enable them to discharge their duties.

2.5 With reference to the above-mentioned documents, the CACSWG identified a total of nine safety-critical core subsystems from the existing ATC system and the new ATC system to be fully commissioned for operational use in October/November 2016. Under the established cyber security management framework, the identified nine core subsystems as listed below should comply with the provisions in the relevant cyber security documents :-

Five Safe-Critical Core Subsystems in Existing ATC System

- Radar Data Processing System & Flight Data Processing System
- Aeronautical Information Database
- Automatic Message Switching System
- ATS Message Handling System
- Speech Processing Equipment

Five Safe-Critical Core Subsystems in New ATC System

- Air Traffic Management System
- Aeronautical Information Management System
- ATS Message Handling System
- Voice Control Switching System
- ATC Data Network

2.6 To prepare for the upcoming transition to the new ATC Centre, SMEs conducted a series of verification tests and inspections on the design and implementation of the new ATC system in 2015 against the cyber security requirements stated in the CCSM and CCSH. In parallel, an external consultant was also engaged to carry out an independent cyber security audit on the ATC data network interconnecting various sub-systems, including penetration test of the external interface system connected to the aviation community. The audit was completed in early 2015 with no anomaly observed. Since late 2015, the CACSWG has been conducting internal audits to verify the compliance to the ATC system access control framework against the CUAMP.

2.7 In May 2016, Hong Kong China engaged a major developer and supplier of Air Traffic Management System (ATMS) to carry out another round of independent assessment on cyber security of the new ATMS and its associated network. The assessment, which was based on relevant international standards, regulations, and industry best practices, revealed that the new ATMS achieved an "Excellent" grading to guard against cyber-attacks, thereby ensuring a safe and reliable system operations.

2.8 The Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force is the government authority responsible for the cyber security of all critical infrastructures in Hong Kong. With the new ATC Centre being classified as a critical infrastructure, the CAD invited CSTCB to conduct an e-Security audit from April 2015 to February 2016, during which the overall design, information flow, network robustness and data integrity of the new ATC system were assessed from cyber security perspective.

2.9 The audit methodology was based on meetings, discussions, documentation review, dataflow and workflow analysis by the CSTCB. Apart from equipment, cyber security readiness of personnel and policy were other major areas being audited. By referencing to common cyber security threats, the audit served to uncover potential security risks that might affect the operation of the new ATC systems of the Hong Kong International Airport in case of an internal or external cyber attack. After assessing all potential risks, the CSTCB concluded that the cyber security provisions and readiness of the new ATC system were satisfactory.

2.10 In line with the CSTCB's recommendation, a direct reporting mechanism was additionally established for CAD to seek swift assistance from the CSTCB in case of cyber attack. To upkeep the cyber security robustness and integrity of the new ATC system, arrangement has been made for the CSTCB to carry out regular e-Security audits in future.

2.11 Hong Kong China has brought forward an important subject of cyber security during the 20th meeting of the CNS Sub-group and the 53rd Conference of Directors General of Civil Aviation. Both meetings note the increasing importance of cyber security for ATC systems. The CNS Sub-

group decided to include a specific agenda item under its standing agenda, and urged States/Administrations to share their experience and lessons learned. During the 53rd DGCA Conference, the Secretary General also remarked that ICAO would consider to bring up this subject in the coming 39th Session of the ICAO Assembly.

2.12 Moreover, managing and combating cyber security threats could only be achieved through the collective efforts among States/Administrations. In fact, the ICAO has been jointly working with ACI, IATA, CANSO, etc on a Civil Aviation Cyber Security Action Plan.

3. ACTION BY THE MEETING

3.1 The Meeting is invited to:

a) note the establishment of an effective cyber security management framework required for a safe and secured ATC system infrastructure;

b) note the latest development and achievements made by Hong Kong, China on implementing cyber security control measures to protect ATC system infrastructure;

c) note that CNS Sub-group would include a specific agenda item on cyber security;

d) seek support from the ICAO in organizing seminars/workshops to discuss, facilitate and exchange experience among States/Administrations, with a view to promoting better understanding of cyber security and planning for implementation of the ICAO Doc 9985 ATM Security Manual; and

e) encourage States to pursue appropriate level of compliance to the cyber security control requirements as stated in the ICAO Doc 9985 ATM Security Manual and make collaborative efforts to effectively address cyber security threats.

— END —