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

WP/31 - Ensuring Cyber Resilience For Air Navigation Service In Hong Kong International Airport And Its Expansion

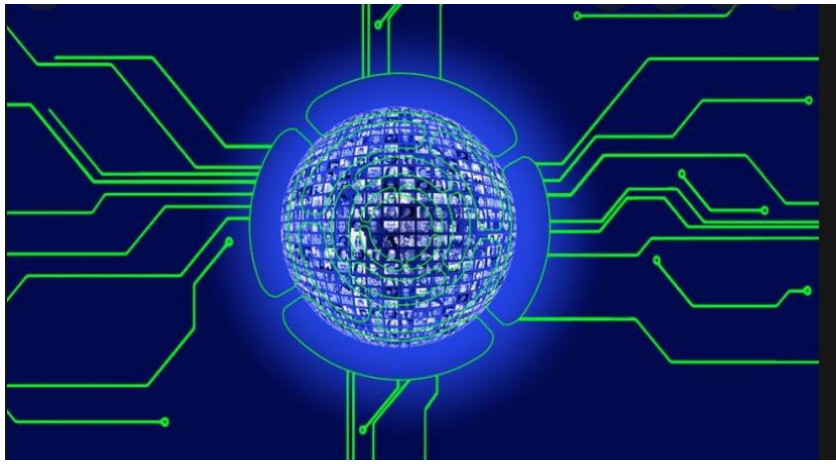
Agenda 12.2

Presented by Hong Kong, China

Introduction

- Increasing **digitization & 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 ICAO's initiative in ensuring cyber resilience in ANS and protecting the ANS critical information infrastructure against increasing cyber security threats.
  - ✓ has established a **cyber security management framework** for pursing compliance with cyber security control requirements stated in ICAO Doc 9985



Cyber Security Policy & Framework Management

- Established a CAD Air Navigation Services Cyber Security Committee (**CACSC**) supported by subject matter experts (SMEs)
  - **Steering** the implementation of cyber security control measures throughout the whole life cycle of ATC system
  - **Containing and mitigating risks** of cyber security threats
  - **Maintaining confidentiality, integrity, availability and safety** in providing air navigation services
  - Conducted thorough analysis for the systems against all applicable cyber security control requirements in **ICAO Doc 9985**

Cyber Security Documentations

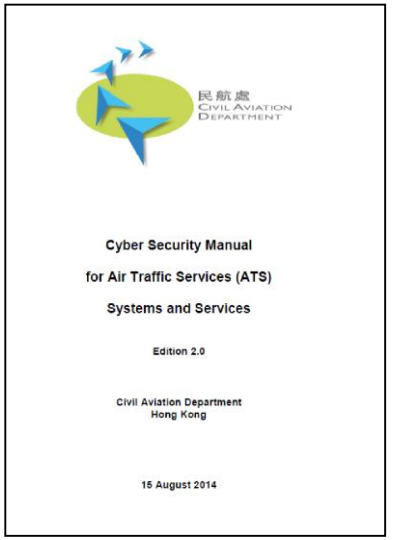
a) CAD Cyber Security Manual for Air Traffic Services (ATS) Systems and Services (CCSM)

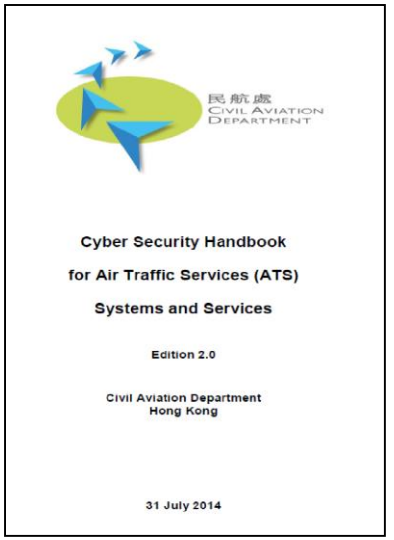
b) CAD Cyber Security Handbook for ATS Systems and Services (CCSH)

c) CAD User Account Management Policy for ATS Systems and Services (CUAMP) and Account Control Framework (ACF)

d) CAD Security Plan for Air Traffic Services (CSP)

e) CAD Project Procedures Handbook (CPPH)





Internal & External Independent Assessments

- Internal assessment on the control measures are conducted regularly, including **verification tests, inspections and audits**.
- Third party organizations are also engaged to carry out **independent assessments** based on relevant **international standards** (e.g. ICAO 9985), regulations, and industry best practices.
- Relevant **recommendations** have been timely implemented.

Collaboration with Cyber Security and Technology Crime Bureau (CSTCB)

- 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 Critical Information Instructure (CII) sectors in Hong Kong
- **CAD invited the CSTCB** to carry out independent assessment and make recommendations on the overall design, information flow, network robustness and data integrity of ANS systems
- The assessment methodology was based on a mixed of on-site/online meetings, discussions, documentation review, dataflow and workflow analysis by the CSTCB; and the cyber security provisions of ANS systems were satisfactory.
- **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.

Cyber Security Incident Drills

- Regularly performed jointly by CAD and HKPF
- Scenarios of terrorists attempting to attack ANS systems was exercised in 2021 to enhance the **incident response capability**.

Photo Credit: Hong Kong Police Force (HKPF)

Expansion of HKIA into Three Runway System (3RS)

- To cope with expansion of 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 the new ANS systems and its associated network in accordance with ICAO Doc 9985 and relevant national standards.
- After assessment, there is **no cyber security risk due to the expansion** and our protective measures (Cyber Security Policy and Framework) **remain effective** in safeguarding ANS systems against cyber attack.

Photo Credit: Airport Authority Hong Kong (AAHK)

Results

- 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.

Conclusion

- Collaborative efforts are important to build a robust and effective cyber security framework
- 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.

Action by the Meeting

- Note the effort of Hong Kong, China in the establishment of an effective cyber security management framework.
- Seek support from ICAO in **organising seminar/workshop to facilitate sharing of experience** among States/Administrations and industry partners
- Encourage to make collaborate effort to **address cyber security threats**


Q
&
A
QUESTION
ANSWER

Thank you


• Safe • Orderly • Efficient
• Airworthy • Teamwork
Committed to a Safe, Efficient and Sustainable Air Transport System