



**ASSEMBLY — 40TH SESSION**

**TECHNICAL COMMISSION**

**Agenda Item 30: Other Issues to be considered by the Technical Commission**

**ATM DATA SECURITY ENHANCEMENTS**

(Presented by the United Arab Emirates)

<b>EXECUTIVE SUMMARY</b>	
This paper presents the work done by the United Arab Emirates regarding security initiatives related to air traffic management (ATM) data within the Middle East (MID) Region.	
<i>Strategic Objectives:</i>	
<i>Financial implications:</i>	
<i>References:</i>	

**1. INTRODUCTION**

1.1 At the Sixteenth MIDANPIRG Meeting held in Kuwait, Decision 26 was the establishment of the ATM Data Security Action Group (ADSAG) to establish a baseline security plan for ATM data services within the MID Region. Subsequent to this the United Arab Emirates has been working, in conjunction with the other MID States, to develop a sound baseline security plan for the Region.

**2. DISCUSSION**

2.1 The ASBU developments (System Wide Information Management (SWIM), Flight and Flow — Information for a Collaborative Environment (FF-ICE), etc.) have been designed to improve efficiency and enable global harmonization throughout the aviation industry. The tangible benefits of these developments do however increase the risks of targeted cyber-attacks on our ATM systems.

2.2 Current ATM systems have very little, if any, security features incorporated into their builds and there are numerous vulnerabilities faced by these systems. Issues such as OS updates/patches that are not maintained by suppliers or the difficulties of enforcing firewall rules for multicast traffic etc., all pose a big risk to the ATM system's security and stability

2.3 ICAO Doc 8973, *Aviation Security Manual*, Chapter 18.1.3 mentions that “States, governments, industry and relevant entities should work collaboratively towards the development of an effective and coordinated global framework for civil aviation stakeholders to address the challenges of cyber threats, and increase the resilience of the global aviation system to cyber threats”.

2.4 As of late 2017 the United Arab Emirates developed the minimum security baseline documents (MSBs) to provide clear and specific requirements for all components of the ATM system, as recommended by Doc 8973, whether the system is connected to the internet or not.

2.5 These documents consist of seven volumes based on ISO 27001 standards and current best practices. These are in no way the final solution for all however they provide a solid foundation and are aimed at being:

- a) easy to implement;
- b) cost effective; and
- c) scalable.

2.6 The seven volumes that make up the MSBs are as follows:

- a) Web Application security baseline
- b) Linux security baseline
- c) Switch security baseline
- d) Application Firewall baseline
- e) Firewall security baseline
- f) Router security baseline
- g) Third Party Data Sharing And Vendor Access

2.7 It is understood that there is a need to include a baseline for radio frequency (RF) security, however RF is generally overseen by State regulatory authorities and they have their own standards/regulations that they follow to ensure the spectrum is protected from interference.

2.8 The MSBs are living documents and are reviewed and updated, where necessary, every six months or when a new update/notification related to one of these documents is received (i.e Cisco security advisory/update).

2.9 After comprehensive reviews and updates the MSBs were endorsed as the baseline security guidelines for the MID Region at the Seventeenth MIDANPIRG Meeting earlier this year (see MIDANPIRG Decision 17/40).

2.10 Additionally to the MSBs the United Arab Emirates has developed a platform which allows all registered users to share knowledge and information as well as a reporting mechanism for cyber events. Having such a platform is imperative as we need to be sharing cyber information to enhance security and the security culture within our industry.

2.11 At the communications, navigation, and surveillance (CNS) SG8 meeting the United Arab Emirates presented the prototype ATM Data and Cyber Security (ADCS) Portal, [www.adcsportal.ae](http://www.adcsportal.ae), and urged users to start registering and providing feedback on enhancements.

2.12 As of April 2019 we launched Version 1.0 of the website with a new and updated Version 2.0 being developed at the same time on our offline test platform.

2.13 As of 1 August 2019 the United Arab Emirates General Civil Aviation Authority has launched Version 2.0 of the website which is a major update and provides an improved reporting mechanism and an enhanced front end. States are urged to register on this site and share knowledge and idea's on improving cyber security within our ATM systems.

2.14 Cyber security is a major challenge within our industry and it is only going to get bigger as new threats emerge. We need to work together and share information and ideas as well as promote a security culture within our industry to provide optimized and stable security measures/policies.

### 3. CONCLUSION

3.1 The Conference is invited to:

- a) urge States to start using the ADCS Portal for the reporting of cyber events and knowledge sharing; and
- b) urge States to provide feedback and suggestions for improvements to the MSB documents and the ADCS Portal.

— END —