SAFETY ALERT 2017-09

Issue 01
Date of Issue: 31st May 2017

SUBJECT:
DEVELOPING CYBER-RESILIENCE WITHIN THE UAE CIVIL AVIATION SYSTEM

REFERENCE PUBLICATIONS:
CAR PART VII AVIATION SECURITY REGULATIONS
CAR PART X SAFETY MANAGEMENT SYSTEMS
CAAP 22 SAFETY INCIDENT REPORTING

REASON:
Following the announcement of the Dubai Declaration[1] on Cyber-security in Civil Aviation during the last ICAO Cyber-Summit and Exhibition hosted by the GCAA in April 2017, awareness about cyber-threats to the aviation eco-system has started to instill within the UAE industry however, the GCAA believes that more guidance must be provided to ensure that the UAE Industry is fortified against this emerging and growing concern.

CAR PART VII AVIATION SECURITY REGULATIONS requires any operator[2] in the UAE to establish measures relating to Cyber Threats. Those measures shall protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation.

It is of high importance that operators dealing with aviation security and safety engage themselves in understanding the safety and security implications that usually fall under the scope of Information and Communication Technology (ICT) Security. ICT Security is part of the wider Security and/ or Safety Management System (SecMS and SMS).

RECOMMENDATIONS:

(a) Operators should ensure that their existing aviation security and/ or aviation safety management systems effectively:
   1) prevent unlawful interference with computerized-systems and equipment (including aircraft's equipment) that are provisioned to assure[3] safe and secure operation of aircraft; and
   2) restrict access of operational data it receives or produces or otherwise employs to those authorised.

[1] The text is available here
[2] 'operator' means any legal or natural person holding a certificate, approval, or any other authorisation granted by the GCAA.
[3] Cyber-security certification audit are one means to assure an acceptable level of protection.

(b) Their management system should define:

1) *the procedures relating to cyber-security risk assessment and mitigation[4], monitoring and improvement, reviews and lesson dissemination;*
2) *the means designed to increase cyber-awareness among their personnel ;*
3) *the means designed to detect cyber-security breaches and to alert personnel with appropriate cyber-security warnings;*
4) *the means of reporting[5] to the GCAA when a cyber-security breach has occurred, even if it was contained; and*
5) *the means of containing the effects of cyber-security breaches and to identify recovery action and mitigation procedures to prevent re-occurrence.*

CONTACT:
regulations@gcaa.gov.ae

[4] A means to achieve effective risk assessment is to conduct vulnerability check and threat modelling.
[5] Preferably use ROSI platform unless the operational data or the IT system falls under the remits of Aviation Security. In such case, use ROSB platform.