



International Civil Aviation Organization

CAR/SAM Regional Planning and Implementation Group (GREPECAS)

Eighteenth Meeting of the CAR/SAM Regional Planning and Implementation Group (GREPECAS/18)

Punta Cana, Dominican Republic, 9 to 14 April 2018

GREPECAS/18 - WP/39

06/04/18

Agenda Item 3: Air navigation activities at global, inter-regional and intra-regional level
3.2 Follow-up on the implementation of global, inter-regional and intra-regional activities

AWARENESS AND TRAINING ON CIVIL AVIATION CYBER SECURITY

(Presented by the Secretariat)

SUMMARY

This working paper presents the relevant information regarding actions taken by the Aviation Security Cybersecurity Programme of the ICAO/LACAC NAM/CAR and SAM Aviation Security and Facilitation Regional Group (AVSEC/FAL/RG). Suggested action is presented in Section 4 of this Working Paper.

References:

- Annex 17, Recommended Practice 4.9.
- Doc 8973/10th Edition - Aviation Security Manual, Chapter 18. Cyber threats to critical aviation information and communication technology systems.
- Doc 9985 - Air Traffic Management Security Manual, Chapter 5. Information and communication technology (ICT) system security (including cybersecurity).
- State Letter NACC71408 dated 24 January 2018, on the Invitation to the Civil Aviation Cyber Security Workshop, (Montego Bay, Jamaica, 20 - 23 March 2018).

1. Introduction

1.1 As the progress of technology and cyber technology is moving forward with a very high speed, cybercrime has escalated around the world affecting different vital areas of organizations, enterprises, financial institutions, communications and even social media. Therefore cyberattacks has turned into one of the emerging threats to critical information and communications technology systems and data, and others involved in civil aviation.

1.2 The ICAO/LACAC NAM/CAR and SAM Aviation Security and Facilitation Regional Group AVSEC/FAL/RG started working on this issue since 2014, and finally as per the Conclusion 7/4 of the AVSEC/FAL/RG/7, held at the ICAO South American Regional Office, from 4 to 6 October 2017, the Cybersecurity Working Group headed by Jamaica completed the development of a training material as guide for the AVSEC/FAL/RG Member States on this issue; and in partnership with the Inter-American Committee Against Terrorism (CICTE) of the Organization of American States (OAS), and thanks to the Jamaican Civil Aviation Authority as the host, a the Civil Aviation Cyber Security Workshop has been conducted in Montego Bay, Jamaica, from 20 to 23 March 2018.

2. Discussion

2.1 The purpose of the workshop was to validate the training material for the Cyber Security Workshop to provide civil aviation regulators, air navigation service providers, airports and aircraft operators, aviation IT support and other aviation industry partners with the basic awareness of cyber security risks. 17 participants from 14 States from the North American, Central American and Caribbean, and South America Regions participated in this workshop that appreciated the developing of such guide to counter this increasing form of attack, and as a potential danger for civil aviation.

2.2 The Inter-American Committee Against Terrorism from the Organization of American States supported with 12 fellowships consisting of air travel and lodge. The Federal Aviation Administration, as well as the Transport Security Administration from United States participated in the event, while Transport Canada participant evaluated the material as part of the validation of the training material for future adjustments.

2.3 The workshop included identifying cyber threats and risks, motives for cyber-attacks as well as a methodology for managing and mitigating cyber-attacks. This awareness Workshop assisted participants on how to be prepared to conduct a risk assessment and prepare a risk management plan on cyber-attacks. The workshop material is designed to assist States in meeting the proposed changes to ICAO Annex 17, current Recommended Practice 4.9 (envisaged to become Standard applicable in November 2018), which will require States to identify critical information and communications technology systems and data used for civil aviation purposes and develop and implement measures to protect them from unlawful interference.

2.4 The Second Phase of this project will include the conduction of a similar workshop for Spanish speaking States, using the same instructors from Jamaica with interpretation, in the last quarter of 2018. Discussions with OAS-CICTE representative were conducted for continuing to support this Cybersecurity project. In the Third Phase of this project, the translation into Spanish of this training material will be considered to conduct a workshop together with a tabletop exercise and if possible with a drill, for the benefit of all AVSEC/FAL/RG Member States.

3. Conclusion

3.1 It will be important for the States raise the awareness on this sensitive matter, and to allocate resources for consider the training of their suitable personnel at all levels of aviation including their Information, Communication Technology (ICT) specialists, taking advantage of the abovementioned developed Cybersecurity Workshop. This will assist to establish a Cyber/Computer Security Incident Response Team (CSIRT) at aviation level, and if possible at national level, and to develop procedures with the national criteria to be executed by a Cyber/Computer Security Emergency Response Team (CSERT) to counter potential attacks to civil aviation.

3.2 Once criteria and procedures are established, and CSIRT and CSERT conformed, exercises on this issue should be considered as part of their contingency plans.

4. Suggested Actions

4.1 The meeting is invited to:

- a) note the content of this working paper; and
- b) ensure the awareness of aviation community on this sensitive matter, and send their participants to future cybersecurity training events.