When replying please quote:
Ref.: NT-NR-7-8 — **E.OSG - NACC74823** 23 August 2018

To: States, Territories and International Organizations

Subject: ICAO NAM/CAR and SAM Workshop on Cybersecurity in Aviation
(ICAO NACC Regional Office, Mexico City, from 4 to 6 December 2018)

Action Required: Please register by 9 November 2018

Sir/Madam,

We are pleased to inform you that, as agreed in the work programme of the ICAO/LACAC NAM/CAR and SAM Aviation Security and Facilitation Regional Group (AVSEC/FAL/RG), the ICAO NACC Regional Office will organize a Workshop on Cybersecurity in Aviation, to be held in its facilities from 4 to 6 December 2018, starting at 09:00 and ending at approximately at 13:00. The working languages will be English and Spanish (simultaneous interpretation services will be provided).

The workshop is open to all ICAO NAM/CAR and SAM States and representatives from the aviation industry (Air Navigation Services Providers –ANSP-, airlines, airports), and is especially oriented to personnel of national authorities responsible for developing related regulation or implementing provisions related to Aviation Security (AVSEC) and Air Navigation Services (ANS).

The objectives of this workshop are to promote common understanding of cyber threats, familiarize participants with the latest developments on cybersecurity, develop a comprehensive view on the subject, and identify best practices by sharing experience and exchanging views.

In order to accomplish these goals, we will gather experts from national appropriate authorities, related International Organizations and technology suppliers who will update the participants through presentations, case studies and discussions.

The Fact Sheet of the workshop is presented in **Attachment A** and contains an outline with the basic information. A more detailed provisional programme of the workshop will be available in early November.

…/2

North American, Central American and Caribbean Office
Av. Presidente Masaryk No. 29 – 3
Col. Polanco V Sección, México City, C.P. 11560, MEXICO
Tel. + 52 55 52503211
E-mail: icaonacc@icao.int
Facebook: @icaonacc
Fax. + 52 55 52032757
Website: www.icao.int/nacc
Twitter: @icaonacc

You are invited to nominate suitable candidates to attend this workshop using the nomination form (**Attachment B** - one per nominee). All nomination forms must be completed in full and authorized by the appropriate authority through official means. The nomination forms must be sent to this Regional Office (icaonacc@icao.int) by **9 November 2018**, in order to enable sufficient time for processing and for selected participants to make travel arrangements, to include visa applications, as necessary. Late nominations, while strongly discouraged, may be considered on a case-by-case basis.

The list of suggested hotels, ICAO NACC Regional Office location, hotel sector maps, as well as other useful information are available on the "Visiting Our Office?" Section of the ICAO NACC Regional Office website (http://www.icao.int/NACC/Pages/visitors_info.aspx). Participants are encouraged to make reservations directly with the hotel(s) in a timely manner.

Accept, Sir/Madam, the assurances of my highest consideration.

for Melvin Cintron
Regional Director
North American, Central American and
Caribbean (NACC) Regional Office

Enclosure:
As indicated

N:\NR - AVSEC-FAL\NR 7-8 - AVSEC Training\1812-CybersecurityWorkshop-MEX\Correspondence\NACC74823AVSEC-States-InvCybersecWorkshop.docx / GGS

ATTACHMENT A

Workshop on Cybersecurity in Civil Aviation

Mexico City, Mexico, from 4 to 6 December 2018

Date:	4-6 December 2018
Location:	Mexico City, Mexico
Duration:	Three working days
Speakers:	Experts from ICAO Member States and organisations in charge of developing policy/implementing provisions related to cybersecurity in civil aviation; representatives from aviation industry (ANSPs, airlines, airports); technology suppliers.
Participants:	Up to 40 participants

Workshop format

The workshop will combine presentations, case studies and discussion. The workshop will encourage and facilitate the exchange of experience and good practices between participants.

Outline and objectives

Cybersecurity incidents are increasing in frequency, magnitude and complexity, and have no border. More interconnection enhances efficiencies and competitiveness, but along with these benefits, new vulnerabilities have emerged. The cloud, where our data are aggregated, makes data more accessible and mobile devices create more entry points for potential attacks.

In this context, Civil Aviation is an increasingly attractive target for adversaries. Although security procedures to date have been effective, the technological advances introduced to airlines, airports and Air Navigation Service Providers (ANSPs) also involve new vulnerabilities and hacking opportunities. Next generation of Air Navigation Service (ANS) systems; tablet-based electronic flight bags (EFB); in-flight entertainment and Wi-Fi connectivity systems; drones; etc. are some of these examples of modernization which improve the efficiency of the civil aviation industry and enhance user experience. How can we implement these advances while ensuring the protection of the civil aviation system against new threats?

Throughout the workshop, participants will:

- develop and promote common understanding of cyber threats, vulnerabilities, and resultant risk across the air transport system;
- identify gaps and improvements in current ICAO cybersecurity Standards and Recommended Practices (SARPs);
- share experience exchange and identification of best practices for a better response and coordination in the event of a cyber-attack.

Who should attend?

The workshop is open to ICAO Member States and civil aviation stakeholders, being of particular interest for:

- Representatives of national authorities responsible for developing regulation or implementing provisions related to Aviation Security (AVSEC) and Air Navigation Service (ANS).
- Experts/managers from airlines, airport operators and appropriate stakeholders responsible for ICT (information and communication technologies) implementation, maintenance of databases and cybersecurity.

Please note: Presentations, workshop material and practical sessions will be conducted in English and Spanish, attendees should have an excellent working knowledge of any of these languages.

— — — — — — — — — — —