International Civil Aviation Organization

A40-WP/348[1]
EX/147
2/8/19

WORKING PAPER

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 12: Aviation Security – Policy

PROPOSAL FOR THE CREATION OF CYBERSECURITY POINTS OF CONTACT (PoC)

(Presented by the Bolivarian Republic of Venezuela)

EXECUTIVE SUMMARY

The Assembly, in Resolution A39-19 *Addressing Cybersecurity in Civil Aviation*, called on member States and industry stakeholders to adopt measures to counter cyber threats to civil aviation, including: the development of a common understanding of cyber threats and risks, coordination between government and industry with regard to aviation cybersecurity strategies, policies and plans, and information sharing to help identify critical vulnerabilities that need to be addressed, as well as to develop and participate in national and international government/industry partnerships and mechanisms for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts. All of the foregoing requires States to develop and implement reliable communication mechanisms to ensure that civil aviation is not disrupted by cyberattacks.

Action: The Assembly is invited to:

Instruct the Council to request that the Secretariat design and implement a network of Cybersecurity Points of Contact (PoC) that quickly, efficiently and securely addresses the global challenges of cyber threats, and implement the specifications in Annex 17 – *Security* to the Convention on International Civil Aviation.

Strategic Objectives:	This working paper relates to the Security and Facilitation Strategic Objective.
Financial implications:	It is proposed that the activities referred to in this paper be undertaken with the resources available in the 2020-2022 Regular Programme Budget and/or from extra budgetary contributions.
References:	Annex 17 – *Security* Doc 10075 *Assembly Resolutions in Force* Resolution A39-19 *Addressing Cybersecurity in Civil Aviation*.

[1] Spanish version provided by the Bolivarian Republic of Venezuela.

1. INTRODUCTION

1.1 The international connectivity of civil aviation entails collaborative work for the development of an effective, coordinated global framework allowing civil aviation stakeholders to address the challenges of cybersecurity. There must also be short-, medium- and long-term measures to ensure the resilience of the global aviation system against cyber threats to the safety of civil aviation.

2. DISCUSSION

2.1 In Resolution A39-19 *Addressing Cybersecurity in Civil Aviation*, the Assembly called on member States and industry stakeholders to adopt measures to counter cyber threats to civil aviation, most notably:

a) encourage the development of a common understanding among member States of cyber threats and risks and of common criteria to determine the criticality of the assets and systems that need to be protected;

b) encourage government/industry coordination with regard to aviation cybersecurity strategies, policies and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed, and;

c) develop and participate in national and international government/industry partnerships and mechanisms for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts. All of the foregoing requires States to develop and implement reliable communication mechanisms to ensure that civil aviation is not disrupted by cyberattacks.

2.2 Another important factor for international coordination relates to the measures that should be implemented when cyber incidents occur that can impact safe and orderly operations in the civil aviation system. Depending on the nature of the incident, communication with the competent authority, the civil aviation authority and systems providers will be critical to ensuring that information can be shared with other users who might be affected, and also prevent further damage by maintaining institutional confidentiality.

2.3 The timely reporting and sharing of specific information can help to delay or prevent similar cybersecurity incidents from impacting other States and industry partners. For that reason, relevant information should be shared as early as possible through pre-established channels or mechanisms.

2.4 States should work with relevant national and international entities to ensure a cooperative approach to reporting system irregularities, suspicious human activity and attacks on data integrity in order to protect critical data and aeronautical information and communications technology (ICT) systems from cyberattack.

2.5 Likewise, all final recommendations and conclusions should be shared with States and aviation industry operators so that they may adjust their respective cyber governance approaches and programmes.

3. CONCLUSION

3.1 All of the foregoing requires States to develop and implement reliable communication mechanisms to ensure that civil aviation is not disrupted by cyberattacks. In view of the specialised nature of security aspects of critical data and ICT systems and the fact that, often, the competent bodies for cybersecurity are not necessarily competent in matters of civil aviation security, the Assembly is invited to instruct the Council to suggest that the Secretariat design and establish a network of Cybersecurity Points of Contact (PoC) that quickly, efficiently and securely addresses the global challenges of cybersecurity threats and implications for civil aviation security.

— END —