International Civil Aviation Organization

A39-WP/17
EX/5
30/5/16

WORKING PAPER

ASSEMBLY — 39TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 16: Aviation Security — Policy

ADDRESSING CYBERSECURITY IN CIVIL AVIATION

(Presented by the Council of ICAO)

EXECUTIVE SUMMARY

International civil aviation is highly reliant on the availability of information and communication technology (ICT) systems, as well as on the accuracy and confidentiality of data, in order to operate efficiently, safely and securely. The protection and resilience of aviation systems against cyber threats and vulnerabilities can only be progressed through a collaborative, harmonized and global approach involving the collective expertise of aviation security, air navigation, ICT security and other relevant communities.

In 2013, ICAO, the Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), the International Air Transport Association (IATA) and the International Coordinating Council of Aerospace Industries Associations (ICCAIA) established an Industry High-level Group (IHLG) as a mechanism for high-level cooperation on issues of common interest and importance, which includes cybersecurity. In that regard, the IHLG determined that cybersecurity in civil aviation was a high priority horizontal issue requiring aligned and coordinated actions by all relevant stakeholders.

In an effort to further promote a consistent and coherent approach in managing cyber threats and risks, ICAO and members of the IHLG developed a draft Resolution as presented in the Appendix to this paper, aimed at addressing cybersecurity in civil aviation through a horizontal, cross cutting and functional approach. The objectives are to reaffirm the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats and obtain global commitment to action by ICAO, its Member States and industry stakeholders, with a view to collaboratively and systemically addressing cybersecurity in civil aviation and mitigating the associated threats and risks.

Action: The Assembly is invited to adopt the draft Resolution on *Addressing Cybersecurity in Civil Aviation*, which is provided in the Appendix.

Strategic Objectives:	This working paper relates to Strategic Objectives A — *Safety*, B — *Air Navigation Capacity and Efficiency* and C — *Security and Facilitation*
Financial implications:	The activities referred to in this paper will be undertaken subject to the resources available in the 2017 – 2019 Regular Programme Budget and/or from extra-budgetary contributions.
References:	*Assembly Resolutions in Force* (as of 4 October 2013) (Doc 10022)

APPENDIX

DRAFT ASSEMBLY RESOLUTION
ADDRESSING CYBERSECURITY IN CIVIL AVIATION

Resolution 16/xx: Addressing Cybersecurity in Civil Aviation

Whereas the global aviation system is a highly complex and integrated system that comprises information and communications technology critical for the safety and security of civil aviation operations;

Noting that aviation sector is increasingly reliant on the availability of information and communications technology systems, as well as on the integrity and confidentiality of data;

Mindful that the threat posed by cyber incidents on civil aviation is rapidly and continuously evolving, that threat actors are focused on malicious intent, disruption of business continuity and theft of information for political, financial or other motivations, and that the threat can easily evolve to affect critical civil aviation systems worldwide;

Recognizing that not all cybersecurity issues affecting the safety of civil aviation are unlawful and/or intentional, and should therefore be addressed through the application of safety management systems;

Reaffirming the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats;

Considering the need to work collaboratively towards the development of an effective and coordinated global framework for civil aviation stakeholders to address the challenges of cybersecurity, along with short-term actions to increase the resilience of the global aviation system to cyber threats that may jeopardize the safety of civil aviation;

Acknowledging the value of relevant initiatives, action plans, publications and other media designed to address cybersecurity issues in a collaborative and comprehensive manner;

Recalling initiatives by the principals of Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), the International Air Transport Association (IATA) and the International Coordinating Council of Aerospace Industries Associations (ICCAIA) and ICAO that recognized the need to work together and be guided by a shared vision, strategy and roadmap to strengthen the global aviation system's protection from and resilience to cyber threats; and

Recognizing the multi-faceted and multi-disciplinary nature of cybersecurity challenges and solutions;

The Assembly,

1. *Calls upon* States and industry stakeholders to take the following actions to counter cyber threats to civil aviation:

    a) Identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems, and the serious consequences that can arise from such incidents;

    b) Define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation;

c) 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;

d) 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;

e) Develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;

f) Based on a common understanding of cyber threats and risks, adopt a flexible, risk-based approach to protecting critical aviation systems through the implementation of cybersecurity management systems;

g) Encourage a robust all-round cybersecurity culture within national agencies and across the aviation sector;

h) Determine legal consequences for activities that compromise aviation safety by exploiting cyber vulnerabilities;

i) Promote the development and implementation of international standards, strategies and best practices on the protection of critical information and communications technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation;

j) Establish policies and allocate resources when needed to ensure that, for critical aviation systems: system architectures are secure by design; systems are resilient; methods for data transfer are secured, ensuring integrity and confidentiality of data; system monitoring, and incident detection and reporting, methods are implemented; and forensic analysis of cyber incidents is carried out; and

k) Collaborate in the development of ICAO's cybersecurity framework according to a horizontal, cross-cutting and functional approach involving air navigation, communication, surveillance, aircraft operations and airworthiness and other relevant disciplines.

2. *Instructs* the Secretary General to:

a) Assist and facilitate States and industry in taking these actions; and

b) Ensure that cybersecurity matters are fully considered and coordinated across all relevant disciplines within ICAO.

— END —