International Civil Aviation Organization

A41-WP/158
EX/72
2/8/22

WORKING PAPER

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

PROVISION OF CAPACITY BUILDING AND CYBERSECURITY TRAINING FOR STATES

(Presented by Guyana and supported by Argentina, Bolivia, Brazil, Colombia, Dominican Republic, Ecuador, El Salvador, Guatemala, Panama, Peru, Uruguay and Venezuela)

EXECUTIVE SUMMARY

Cybersecurity is a multidisciplinary phenomenon that remains a threat to civil aviation. ICAO has recognized this threat to international civil aviation security and has developed its Cybersecurity Strategy and Cyber Security Action Plan in response. Whilst these policies and guidance materials are beneficial to States, it is imperative that States are equipped with the relevant knowledge, capability, training and resources to effectively mitigate cyber threats and risks nationally, regionally and internationally.

This working paper is therefore requesting that ICAO dedicate resources towards capacity building for States to satisfy the objectives of its Cybersecurity Strategy's Seven Pillars which are outlined accordingly:

a) International Cooperation;
b) Governance;
c) Effective legislation and regulations;
d) Cybersecurity Policy;
e) Information sharing;
f) Incident Management and Emergency Planning; and
g) Capacity Building, Training and Cybersecurity Culture

Action: The Assembly is invited to:

a) Direct the Council to request the Secretariat to dedicate resources towards Cybersecurity resilience and capacity building for small States. Some of the areas of need are cybersecurity awareness training; cybersecurity incident management and emergency response training and cybersecurity instructors training and certification training programme; and
b) ICAO to promote and create cooperation mechanism to foster aviation mentorship and technical exchange programmes among States.

Strategic Objectives:	This working paper relates to the *Security and Facilitation* Strategic Objective.
References:	Annex 17 – *Aviation Security* *Aviation Cybersecurity Strategy* *Cybersecurity Action Plan*

1. INTRODUCTION

1.1 Civil aviation air traffic is projected to increase and so will its reliance on technology. Greater reliance on technology leads to greater threats and risks that makes cybersecurity an important issue for States and the need to build resilience against its threat. Cybersecurity in aviation is imperative, as it exists on a broad-spectrum, which involves aspects of safety, security, air navigation, ICT systems and general aviation operations. The ICAO Cybersecurity Strategy and Cybersecurity Action Plan provides the necessary guidance for States to start setting a foundation to build a robust cybersecurity infrastructure. However, this will require capacity building, training, cybersecurity culture and inter-agency and inter-regional collaboration.

1.2 In order to build a robust cybersecurity infrastructure, States are required to follow the seven pillars of the ICAO Aviation Cybersecurity Strategy and adopt the ICAO Cybersecurity Action Plan which sets the foundation for States, industry stakeholders and ICAO to collaborate to develop the ability to identify, prevent, detect, respond to and recover from cyber-attacks on civil aviation as well as create a framework for cooperation. The Cybersecurity Action Plan proposes several measures and actions that States should adopt to satisfy the objectives of the seven pillars. These are inclusive of international cooperation amongst States, establishment of governance structures, drafting of effective national legislations and regulatory frameworks, developing cybersecurity policies, sharing relevant information amongst States, incident management and emergency planning and capacity building, training and promoting a cybersecurity culture ultimately to build resilience to address this global phenomenon.

1.3 Building capacity is essential for the establishment of a robust cybersecurity (global) infrastructure. It is the foundation upon which the other six pillars can be achieved. Hence, ICAO is urged to foster and provide the necessary capacity building for States especially small States.

2. DISCUSSION

2.1 Guyana has taken several initiatives to combat cyber-attacks and to build cybersecurity resilience, which are in alignment with the seven pillars of the cybersecurity aviation strategy. This mission is headed by the National Data Management Authority (NDMA) which is the entity designated for the monitoring and protection of data within Guyana. The NDMA has commenced the drafting of National Cybersecurity Policies, Standards, Legislations and Regulations that are promulgated for consultation through inter-agency committees. This is an iterative process that requires input from the relevant agencies, particularly of those with critical infrastructure. Given the limitations and challenges of small States, there is a need for the provision of external guidance and training on how to address cybersecurity holistically. Even though information is shared nationally amongst agencies and training is solicited through the inter-agency committee, capacity building as a State is necessary.

2.2 Capacity building entails the provision of relevant training for aviation personnel to increase their knowledge, proficiency, skills and capabilities in cybersecurity. It also entails the provision of the relevant human and capital resources to build a robust cybersecurity infrastructure. It requires qualified and experience personnel to draft legislation and regulations on cybersecurity. This capacity can be built through the execution of national, regional and international workshops. It requires relevant and adequate training to strengthen the capabilities of States to manage cybersecurity incidents and emergency response planning. This is imperative as cyber-attacks cannot be stopped in its entirety but can be mitigated with robust systems. Hence, cyber-attacks will happen, but it is essential that the States are capable of building resilience for business continuity.

2.3 The provision of training sessions, workshops, apprenticeships programmes and mentorship programmes etc., are necessity to build capacity for small States. These can be provided to individual States and to the Region, as the case requires.

3. CONCLUSION

3.1 This working paper recognises the need for States to building capacity building and strengthen cybersecurity resilience.

— END —