**Twenty-Second Meeting of the AFI Planning and Implementation Regional Group (APIRG/22)**
**(Accra, Ghana, 29 July – 2 August 2019)**

# UPDATE ON THE PROGRESS IN CYBERSECURITY

*(Presented by the Secretariat.)*


| SUMMARY | |
|---|---|
| This information paper presents an update on the ongoing cybersecurity work of ICAO and provides information related to a Cybersecurity Strategy Draft Assembly Resolution, as well appropriate cybersecurity awareness and training<br><br>Action by the Meeting is invited to note the information provided. | |
| *Strategic Objectives:* | Safety and Efficiency |


## 1 INTRODUCTION

1.1 The 39th Session of the ICAO Assembly reaffirmed the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber-attacks and obtain global commitment for action by ICAO, its Member States and industry stakeholders, with a view to collaboratively and systematically addressing cybersecurity in civil aviation and mitigating the associated threats and risks. Resolution A39-19, Addressing cybersecurity in civil aviation, identified the actions to be undertaken by States and other stakeholders in this regard. The 39th Session of the ICAO Assembly also instructed ICAO to develop a comprehensive cybersecurity work plan and governance structure.

1.2 To meet these objectives, ICAO established the Secretariat Study Group on Cybersecurity (SSGC) under the lead of the Deputy Director, Aviation Security and Facilitation (DD/ASF). The SSGC is monitored by the Secretariat Senior Management Group on common safety and security issues, chaired by the Secretary General of ICAO.

1.3 Since its establishment in August 2017, the Secretariat Study Group on Cybersecurity (SSGC) has met six times and has produced a proposal for a strategy for cybersecurity in civil aviation, which will be presented to the 217th Session of the Council (C-WP/14865 refers).

1.4 The Second High-level Conference on Aviation Security (HLCAS/2) produced a set of recommendations in support of a Cybersecurity Strategy, and the possible establishment of a Cybersecurity Panel.

## 2. DISCUSSION

*Progress report of the SSGC*

2.1 The SSGC held its sixth meeting in Tel Aviv, Israel on 21 March 2019. The meeting was held in conjunction with the second meeting of its Research Sub-Group on Legal Aspects; the third meeting of its Working Group on Aerodromes; and the second meetings of its Working Groups on Airworthiness, and Current and Future Air Navigation Systems.

*Research Sub-Group on Legal Aspects*

2.2 The Research Sub-Group on Legal Aspects (RSGLEG) considered whether a new or updated survey on the national legislation, policy and practices of States would be needed to facilitate its work. It furthermore considered the legal approach to certain aspects regarding preventive and remedial measures to deal with cyber threats, including:

a) reporting and information sharing between States and within States between responsible agencies and industry organizations;

b) protection for cyber vulnerability research and testing;

c) supporting business continuity and recovery from disruption following a cyber-attack; and

d) means for legal attribution of cyber-attacks.

2.3 The meeting supported the establishment of a repository of national legislation dealing with cybersecurity for civil aviation, and suggested that this repository could be developed and made available by ICAO.

*Working Group on Aerodromes*

2.4 During its deliberations, the working group concluded that a centralized repository for cybersecurity guidance should be established, and that consideration will need to be given to the access conditions of such – including questions of restrictions and revenue generation. It was suggested that Chapter 18 of the ICAO *Aviation Security Manual* (Doc 8973, Restricted) should be extracted and made available in an unrestricted but expanded manner.

2.5 The Working Group identified a need to establish sharing mechanisms for relevant and appropriate information on cybersecurity issues. As a prerequisite for such a mechanism, a clear definition of “cyber threat” would need to be developed.

*Working Group on Airworthiness and Working Group on Current and Future Air Navigation Systems*

2.6 The groups agreed on the need for a common cybersecurity lexicon, specifically with regards to the draft cybersecurity strategy, to eliminate confusion with any terms. While it was understood that some terms may well have varying definitions depending on the use and circumstances, there should be clarity with respect to ICAO’s use and understanding of them, and the groups encouraged the use of European Civil Aviation Conference (ECAC) Doc 30 Recommendations on cyber security and supporting Guidance Material as a suitable basis to model this terminology.

*Cybersecurity Strategy*

2.7 Since its inception in August 2017, the SSGC has met six times and developed a set of recommendations to address the emerging issue of cybersecurity in aviation. The principal outcome was the development of a comprehensive cybersecurity strategy. The strategy aims to steer the work of States and ICAO with the aim of ensuring the safety, security and continuity of civil aviation through the application of a robust cybersecurity framework.

2.8 The Council considered the strategy on the basis of C-WP/14865 (Revision No. 1), which presented a comprehensive cybersecurity strategy and a related Assembly Resolution. The Council also had for consideration an oral report thereon from the Committee on Unlawful Interference (UIC).

2.9 It was recalled that this item had been discussed during the previous session of the Council, following which the SSGC had developed the comprehensive strategy that was now being presented for consideration. In this connection, it was noted that the UIC had agreed in-principle with the content of the proposed strategy, but that questions had been raised in terms of the process by which this should be conveyed to the Assembly. One option was for the strategy to be presented in the form of a new Assembly Resolution to complement the existing Assembly Resolution A39- 19 "Addressing Cybersecurity in Civil Aviation", while the second option proposed that the existing Assembly Resolution A39-19 be amended to incorporate references to the strategy. Following consideration, the Council agreed to proceed with the second option since this would allow for a more coherent and uniform approach.

2.10 In relation to the action paragraph of the draft Assembly working paper, the Council agreed that this should be amended so that it would read: "The Assembly is invited to:

a) endorse the Cybersecurity Strategy as approved by the Council;

b) adopt the proposed Assembly Resolution that supersedes Assembly Resolution A39-19; and

c) urge States to ratify the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft*".

2.11 In addition, in relation to the second operative clause of the draft Assembly Resolution, the Council decided to amend the text so that it would now read: "Calls upon States and industry stakeholders to take the following actions to counter cyber threats to civil aviation:

a) Implement the Cyber security Strategy;

2.12 The Strategy highlights the importance of recognizing cybersecurity as a cross-cutting issue that involves all domains of the aviation sector. It synthesizes existing provisions that relate to cybersecurity issues that are spread across the various Annexes into a single framework, focused on the management of cyber risk and improving cybersecurity as a whole. The Strategy provides States with a vision of the civil aviation sector as resilient to cyber-attacks, whilst continuing to innovate and grow.

2.13 The strategy aims for:

a) the protection of civil aviation and the travelling public from cybersecurity threats that might affect the safety, security and trust of the air transport system;
b) maintaining or improving the safety and security of the aviation system in preserving the continuity of air transport services;

c) States to recognize their obligations under the Convention on International Civil Aviation (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cybersecurity threats; and

d) coordination of cybersecurity measures among State authorities to ensure effective and efficient management of cybersecurity risks.

*Future working structure for cybersecurity at ICAO*

2.14 The Council during its 215th Session requested that the Secretariat conduct a feasibility study for the possible creation of a Cybersecurity Panel. The HLCAS/2 recommended that ICAO should commence a feasibility study for the establishment of a Cybersecurity Panel with a clear timeframe, without delaying the ongoing work of the Secretariat Study Group on Cybersecurity (C-WP/14825).

2.15 Based on the discussions in the SSGC, and considering other ongoing initiatives related to cyber-security, the Secretariat has outlined five different scenarios for how the work on cyber-security could progress: Establishment of a Cyber-Security Panel under the Unlawful Interference Committee; Establishment of a Cybersecurity Panel under the Air Navigation Commission; Establishment of a working group on cybersecurity under the Aviation Security Panel; Evolution of the SSGC; and Establishment of a Task Force on Cybersecurity.

2.16 The aforementioned five scenarios were presented to Council during its 217th Session for deliberation and consideration.

2.17 Following consideration, the Council:

a) welcomed the progress that had been made by the Secretariat Study Group on cybersecurity;

b) requested the Secretariat to undertake a comprehensive feasibility study and gap analysis in order to more clearly identify what mechanism is most appropriate to address the issues in cybersecurity in civil aviation; and

c) further requested that the outcome of this work by the SSGC would be presented at a future session of the Council, with an interim progress report to be presented at the 218th Session (November 2019).

*Cybersecurity awareness and training*

2.18 Cybersecurity continues to be of great interest and concern at the global and regional level. Various regional awareness and training events in form of workshops, seminars and training courses have started to evolve through initiatives by States and the ICAO Regional Offices. At the same time different training organizations of the TRAINAIR PLUS Progamme wish to start the development of

relevant cybersecurity training courses.

2.19 ICAO supports these regional and national initiatives and recognizes the demand for cybersecurity awareness and training events and programmes. An important factor in the future development of all these initiatives is the harmonization of such activities and alignment with the ICAO Cybersecurity Strategy.

2.20 To this end ICAO has decided to develop a cybersecurity briefing and awareness package that will be made available to the Regional Offices ahead of the Assembly, and which will provide harmonized introductions and information to ICAO's view on cyber-security and include a comprehensive overview of the organization's cybersecurity work.

2.21 In a further step, ICAO's Aviation Security and Facilitation Branch (ASF) is working with the Global Aviation Training Office (GAT) to develop a cybersecurity training package. This package will be based on the outline already developed and approved by the AVSEC Panel.

2.22 At the same time, ASF and GAT are finalizing a new training package on Air Traffic Management (ATM) Security in collaboration with EUROCONTROL. The intention is for this package to mirror existing provisions and guidance materials on this subject, including those contained in ICAO Doc 9985, *Air Traffic Management Security Manual* (2013).

*Other ICAO initiatives and projects related to cybersecurity*

2.23 Following discussions and recommendations of the SSGC and its working groups, ICAO began the development of a cyber-security repository that would serve a centralized exchange platform for guidance material, best practices and outcome of cyber-security exercises for States and industry. The platform would also incorporate a dedicated communication and contact platform for cybersecurity experts from States and industry, in order to facilitate the exchange of relevant information and develop a cybersecurity "social" network.

2.24 In line with another ICAO initiative which was initially deliberated in the AVSEC Working Group on Innovation and will be presented at the upcoming Aviation Security Panel meeting aiming for the integrated collection of safety and security information – referred to as iSHARE – ICAO continues to explore how cybersecurity relevant information could be integrated as well.

## 3 ACTION BY THE MEETING

3.1 The meeting is invited to note the information provided.

— END —