IIM/SG/4 WP4.2E

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Fourth Meeting of the APIRG Infrastructure and Information Management Sub-Group (IIM/SG4)

(Virtual, 10-13 August 2021)

Agenda Item 4: ***Status of implementation of the regional projects***

WP4.2E - Progress report of IIM SG COM 5 project "Assessment of AFI Air Navigation Services Cyber resilience"

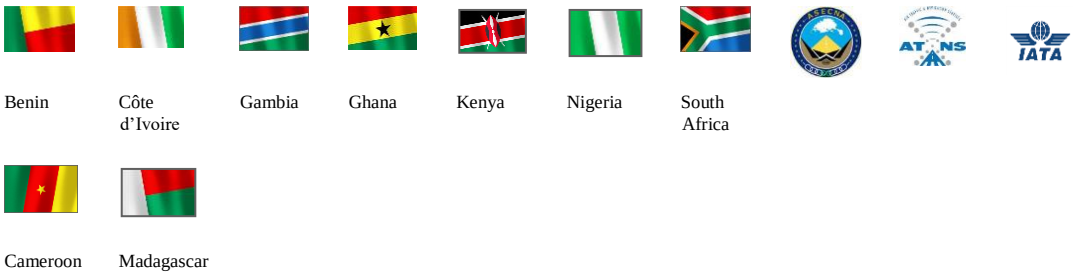
(Presented by Côte d'Ivoire)

SUMMARY
This working paper outlines the progress of IIM SG COM 5 project "Assessment of AFI Air Navigation Services Cyber resilience" and the challenges encountered. Action by the meeting in paragraph 3
REFERENCE(S): ▪ Global Air Navigation Plan (GANP) ▪ Report of the 3rd meeting of IIM SG (APIRG IIM SG/4) ▪ ICAO Aviation Cybersecurity Strategy ▪ ICAO Cybersecurity Action Plan
This working document relates to ICAO Strategic Objectives: A – Safety and B – Air Navigation Capacity and Efficiency. **KPIS and concerned ASBU B0 Modules:** All applicable to CNS and Spectrum.

1. INTRODUCTION

1.1. The IIM SG COM 5 Project was launched end 2017 to address cyber safety, and cyber resilience of air navigation and information management systems in AFI region.

1.2. The project team is composed of ICT, cybersecurity and ANS experts from AFI States and organizations:



Benin, Côte d'Ivoire, Gambia, Ghana, Kenya, Nigeria, South Africa, Cameroon, Madagascar

1.3. This paper provides the progress made by the IIM Masterplan project. It elaborates the achievements, challenges encountered by the team, possible recommendations.

2. DISCUSSIONS

2.1 Scope

2.1.1 The objectives of the IIM COM 5 project are to:

- assess the cyber threats on Air Navigation systems.
- promote cyber safety and resilience culture in the AFI Region among the stakeholders:
  - CAAs in charge of ANSPs oversight,
  - ANSPs providing the services which need to be protected against cyber-attacks and
  - counter parts operating in the vicinity of airport (such as airlines, airport operators,.) that can interact with software that can affect ANS in terms of cyber risks.
- develop a cyber resilience framework (guidelines) for voluntary use by AFI ANSP organizations / member states to:
  - harmonize the way cyber resilience and safety are implemented and
  - build capacity for each member state in developing ANS cyber resilience policy.

2.2 Actions conducted (Key achievements)

2.1. Project documentation

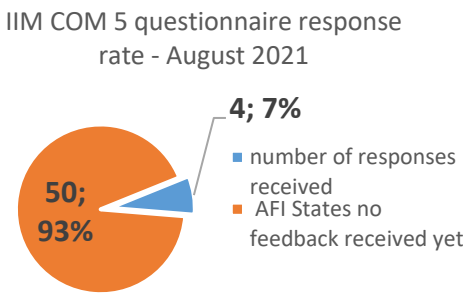
2.2. All project initiation/planning documentations (Project Description, Terms of Reference, and Organization/Plan), submitted in 2019, had been updated in 2021 (attached as Annexes A, B and C).

2.3. The project linkage matrix and the project cost estimation are under development and should be finalized by end of September 2021.

2.4. A collaborative platform had been set up for the project on Microsoft teams to share all project conversations, files, deliverables.

2.5. Assessment of current cyber resilience of ANS in AFI region *(project baseline questionnaires)*

The key challenge faced by the project is related to the project questionnaire survey and State responses (few responses received so far).



2.2.1 AFI ANS Cyber safety and cyber resilience framework

2.2.1.1 As a reminder, the AFI ANS Cyber safety and resilience framework provides general guidelines on how to assess the cybersecurity risks, threats and vulnerability to Air Navigation Services and methods of mitigating such risks. This framework is based on Aviation Cybersecurity Strategy and the proven cybersecurity standards and frameworks (ISO 27000 series, NIST, etc.

2.2.1.2 The ANS Cyber safety and resilience framework, submitted to IIM Subgroup Chairman and Secretariat in February 2020, is being updated to ensure alignment with the Aviation Cybersecurity Strategy, the ICAO cybersecurity action Plan, and the current aviation cyber safety initiatives (considering what is relevant/appropriate for AFI region).

2.2.2 ANS Cyber safety and resilience awareness campaign

2.2.2.1 The project team is developing a communication plan to raise awareness on cyber safety and resilience.

2.2.2.2 This communication plan will include:

- A selection of few Short and key messages on Cyber safety / resilience of Civil aviation, to be displayed on one slide format. Those messages could be shared on ICAO website (see IIM SG Secretariat).
- Development of e-flyer on cyber basic advice, cyber security awareness posters, visual contents.

2.3 **The way forward** *(Outlook for the next reporting period)*

2.3.1 **Goal 1: "Make things more concrete":**

2.3.1.1 the project team organized several meetings with the industry (with extensive expertise in air traffic management and aviation cybersecurity).

2.3.1.2 With the assistance of the industry, or other partnership toward the world, the following actions/tasks had been identified and will be planned during the 2nd semester 2021:

a) build concrete cyber-attacks scenarios that will trigger the needs for specific reactions among organizations/states, through cyber-attack scenario simulation
b) provide real examples of cyber-attacks (combination of IT and OT approaches).
c) conduct seminars or webinars (for instance for top managers), share the cybersecurity culture, training, sensitize people (how educate people and be aware of the threats) and capacity building on response to cyber threat on computers systems supporting ATM operations

2.3.2 Goal 2: "Finalize the core project activities" by November 2021: framework and assessment of current AFI ANS cyber resilience

d) Update the AFI ANS Cyber safety and resilience with latest input/information from ICAO Working Group on Air Navigation Systems (WG-ANS) of the ICAO Secretariat Study Group on Cybersecurity (SSGC), CANSO, IATA, EUROCONTROL initiatives.
e) finalize project baseline questionnaire survey (more responses needed).
f) Finalize linkage between IIM and AAO projects
g) Develop project cost estimation before the next APIRG meeting

2.3.3 **Goal 3: "Communicate on ANS Cyber resilience (to raise awareness)" by October 2021**

3. ACTIONS BY THE MEETING

3.1 The meeting is invited to:

a) Take note of the progress made so far by the project team and the challenges.

b) Encourage State participation in the AFI region projects.

c) Support concrete actions already taken or underway by States and organizations to respond to cyber-attacks targeting computer systems that support ATM, and

d) Submit projects Questionnaire responses.

.

----- FIN -----