INTERNATIONAL CIVIL AVIATION ORGANIZATION

WESTERN AND CENTRAL AFRICA OFFICE

Twenty-seventh Meeting of the AFI Satellite Network Management Committee (SNMC/27)
(Accra, Ghana Faso, 25-29 November 2019)

Agenda Item 5: Cyber Safety and Resilience

Regional initiative on Cyber Safety and Resilience of ANS systems

(Presented by the Secretariat)

SUMMARY

This paper provides the meeting with the outcome of initiatives taken in the region to address Cyber Safety and Resilience of ANS systems

Reference: **APIRG Report**
SNMC 26th Report
SAT/24 Reports

Action by the meeting in Paragraph 3

1. INTRODUCTION

1.1 The SNMC 25th meeting (**Freetown, Sierra Leone, 18-22 December 2017)** under its agenda item 5, discussed the outcome of APIRG 21st Meeting and addressed issues related to the Cyber Safety and Resilience of AFISNET.

1.2 The meeting called upon ANSPS under (*Conclusion 25/19*) to:
a) Conduct Gap analysis to identify AFISNET cyber vulnerabilities and mitigate the related risks;
b) Consider the protection of AFISNET against cyber threat in the technical specification;
c) Provide with the support of ICAO, technical and operational personnel with the adequate education training in the matter.

1.3 The meeting also decided (*Decision 25/20)* to expand the mandate of the Joint Technical Team for AFISNET re-engineering and modernization to address issues on Cyber Safety and resilience of AFISNET

2. DISCUSSION

2.1 The issues on Cyber Safety and Resilience of the air navigation system has been addressed at the regional level by APIRG under APIRG COM Project 5: Assessment of AFI Aeronautical Networks Cyber Security. With the objectives to:

- Implement a cyber-security policy over the AFI region, which would assess all issues including the definition of common threats scenarios, training, performances, security studies, audits and controls.
- Assess the cyber issues on all systems and networks if the analysis has not yet been made
- Implement a systematic process of cyber risk evaluation on all new systems
- Assess and prevent internal and external threats impact the availability, the reliability, the integrity and the continuity of the AFI aeronautical networks, including RFI

2.2 The project is organized as following:

- **Project Team Coordinador**: *Côte d'Ivoire (***Ms Sandrine Gnassou***)*
- **Project Team Experts**: *Côte d'Ivoire, Benin, Gambia, Ghana, Kenya, Nigeria, South Africa, ASECNA, IATA*

2.2 The project adopted a Strategy consisting on:

- Assessing the current aeronautical networks security and diagnostic the potential threats to the safe provision of the air navigation service in the AFI region
- Implementing a comprehensive security policy for a secured operation of the AFI systems and networks
- Training and qualification of Technical and operational staff
- Appointing ICAO and Designated Experts to conduct Technical workshops to support the development of the project

2.3 The project has been working successfully since its approval by APIRG through teleconferences and has delivered the programme attached in **Appendix**.

In order to enhance the awareness of States experts on the issue a regional workshop is being convened next week in Nairobi.

3. ACTION BY THE MEETING

The meeting is invited to:

- Take note of the information provided above on the regional project on the Assessment of AFI Aeronautical Networks Cyber Security

- Make any proposal to expedite the implementation of the strategy for Aeronautical Networks Cyber Security and agree on future activities there on.

— END —

Activities & Outputs

1. Initial tasks (set by IIM Chair)

The IIM Sub Group teams were allocated the following tasks and expected to deliver as indicated in the table below:

N°	TASK	RESPONSIBLE	PLANNED DUE DATE	COMMENTS
1	Project team coordinators and experts appointment finalization	States / Organization	31/11/2017	The project team coordinator had been officially appointed by Côte d'Ivoire. ASECNA had officially appointed M. Cumbi, M. Sougue and M. Amegboh. The list of all the experts appointed had not been communicated yet.
2	Project Team Organization	Project Coordinators	31/12/2017	Has been finalized and sent to IIM Sub-Group Chair, Vice and Secretariat on 31/12/2017 (Edition 00.00.01). An updated edition of the document has been sent on 25/06/2018
3	Project ToR	Project Coordinators	31/12/2017	Has been finalized and sent to IIM Sub-Group Chair, Vice and Secretariat on 25/06/2018
4	Project link finalisation	Project Coordinators	31/10/2017	Has been finalized and sent to IIM Sub-Group Chair, Vice and Secretariat on 20/04/2018
5	Project Questionnaire	Project Coordinators	31/12/2017	Has been finalized and sent to IIM Sub-Group Chair, Vice and Secretariat on 31/12/2017 (Ed 00 00 03). An updated edition of the document has been sent on 25/06/2018

2. Project technical tasks (set by IIM SG COM Project 5)

The IIM SG Communication Project 5 was initiated on 22nd of December 2017 via Skype meeting. Due to technical issues, all the project members did not achieve to join the Skype meeting. Therefore, a second kick off meeting had been organized on 28th of February 2018 via Skype meeting.

In the project organization description document, the following tasks had been identified to meet the project objectives. The table below provides the progress for each task/activity/deliverable.

Project Deliverables	Planned Date of Delivery	Objectives	Status[1]	Actual date of completion	Progress
[D01] Project Description	31/12/2017	To provide a description of the project	Achieved	29/012/2017	Has been sent to IIM Sub-Group Chair, Vice and Secretariat
[D02] Organization of project team	31/12/2017	To set the basis for the project organization and coordination	Achieved	29/012/2017	Has been sent to IIM Sub-Group Chair, Vice and Secretariat
[D03] Terms of reference	June 2018		Achieved	25/06/2018	
[D04] « Cybersecurity in Civil Aviation Operational concept description »	October 2018	To share a common understanding of cyber, common definitions of cyber (cyber threats, cyber risks cyber resilience, cyberattacks, cyber culture)	In progress		A first draft had been distributed to the project team for review . There is a need to agree on a task allocation in order to be more efficient
[D05] List of AFI Aeronautical Networks	September 2018	To have a full list of aeronautical networks in AFI Region	In progress		Under development

[1] Achieved in progress Challenges Not started

Project Deliverables	Planned Date of Delivery	Objectives	Status[1]	Actual date of completion	Progress
[D06] Assessment of the current aeronautical networks cyber security and diagnostic of the potential threats to the safe provision of the air navigation service in the AFI region	November 2018	To assess the current aeronautical networks security and diagnostic the potential threats to the safe provision of the air navigation service in the AFI region	Not started		
[D07] Global cyber security policy for a secured operation of the AFI systems and networks	February 2019	To define the global cybersecurity policy for aeronautical network in AFI region	Not started		

Project Deliverables	Planned Date of Delivery	Objectives	Status[1]	Actual date of completion	Progress
[D08] Teleconferences, Workshops/Seminars, working sessions (French and English) on global cyber security policy	TBD	Working Sessions are an essential tool to: • Discuss with main African Stakeholders about key essential aspects of Cybersecurity in Aviation • Network people and contribute to build capacity in Cybersecurity in aviation • Deliver valuable information to decision makers about Cybersecurity • Gather best practices from other regional initiatives on Cyberspace issues for Aviation	Not started		
[D09] Feasibility study of setting up an AFI Regional Operational Centre for Cybersecurity in Aviation on a long term basis	October 2019	To assess the feasibility of setting up of an AFI regional Centre for Cybersecurity in Aviation	Not started		

3. Challenges & Lessons Learned

The following table summarizes the challenges we have faced during the reporting period and the lessons learned / solutions for each challenge.

Challenge	Lessons learned / solutions
List of IIM COM 5 Project team members	There is an urgent need to confirm the participation of the experts that had been appointed to the project (and to encourage their participation).
Participation	Because of the delay in finalizing project team appointments, there was a lack of participation of the project team, at the beginning of the project. The participation remains an important issue as the success of the project will rely on all the experts 'contributions and participation (by emails, to the meetings). The next IIM meeting will help to strengthen the project team group cohesion and motivation.
Coordination and Communication Difficulties	The project team experienced a lot of technical network challenges (Teleconference, GoToMeeting, Skype). • Most of the meetings had been cancelled because the project members were not able to connect to the skype meeting. There is a need to find a more reliable means for the online meetings. • we encounter many difficulties in organizing project progress meetings. Some participants, although motivated, cannot connect to skype meetings. This is undoubtedly a technical problem independent of the IIM or ICAO sub-group, but it is a permanent obstacle to the good conduct of the project. Therefore, It would be interesting to gather tips and best practices from other IIM or AAO projects, or any other project (any other means of communication (WebEx, physical meeting)).

Challenge	Lessons learned / solutions
	As IIM COM Project 3, a decision to communicate via WhatsApp had been taken (for IIM COM Project 5).
Information sharing between the IIM project	IIM projects work in parallel with difficulties or successes. It would be interesting to collect the difficulties and good practices in order to share them with all the project coordinators. In addition, periodic meetings between the IIM project coordinators and the IIM Chair should be organized.
Confidentiality	For the cybersecurity subjects, the IIM Sub group should define confidentiality requirements. Some information should be protected