



ICAO

UNITING AVIATION

NO COUNTRY LEFT BEHIND



“AFI Air Navigation Services Cyber safety and resilience assessment”

IIM SG COM 5 Project Progress status – August 2021

Presented by Sandrine GNASSOU - Project Coordinator (Côte d'Ivoire)





AGENDA



- 1** Introduction

- 2** Discussion
 - 2.1 Scope
 - 2.2 Actions undertaken
 - 2.3 Challenges and Solutions
 - 2.4 Way Forward

- 3** Action by the Meeting
 - 3.1 The meeting is invited to...
 - 3.2 Draft Conclusion/Decision That :
.....
.....

Attacks on Aviation are happening...

(*) source : *EUROCONTROL Think paper #12*

<https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cybercrime>



COVID 19 HAS TRIGGERED A WAVE OF CYBER-ATTACKS HITTING THE AVIATION INDUSTRY*

CYBER CRIMES COST AVIATION **BILLIONS** EVERY YEAR*



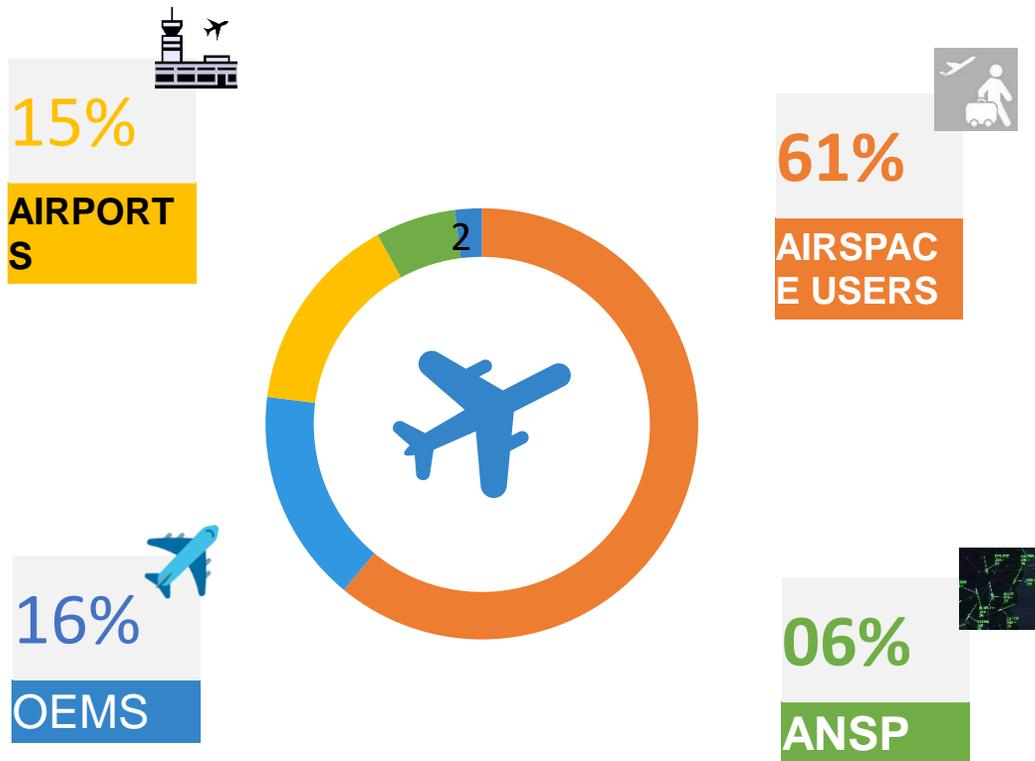
ONE BIG RANSOMWARE ATTACK **EVERY WEEK ON AVIATION***



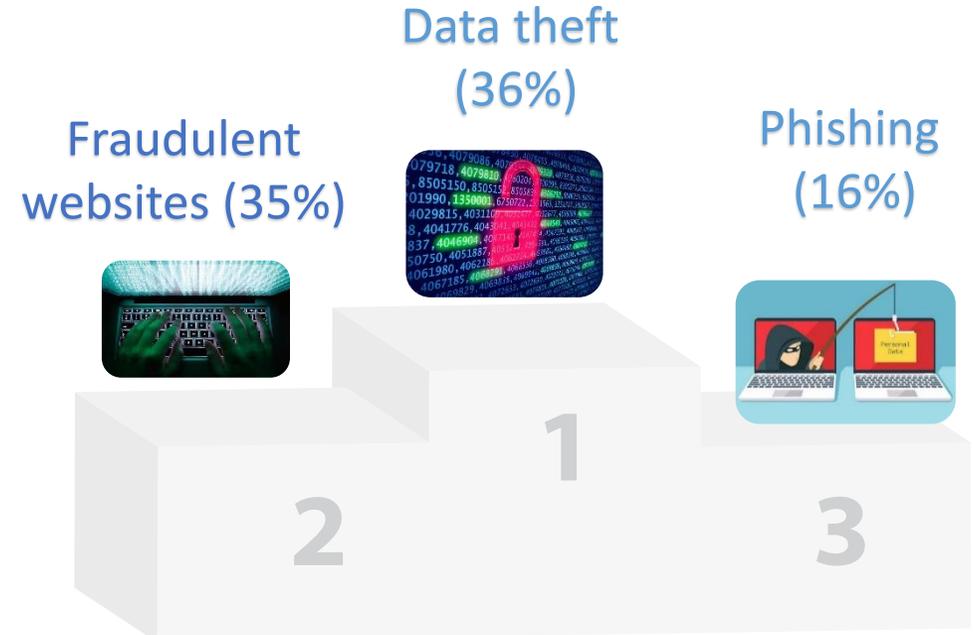
2021 - Aviation cyber threat landscape – Europe (~1260 events*)

(source : [Eurocontrol 2021 report on cyber on aviation](#))

2020 Aviation Cyber attacks surface



2020 Top 3 : Aviation cyber attacks types



IIM SG COM 5 project is addressing AFI Air Navigation Services cyber safety & resilience

Project Objectives



Project Members

ANS, CNS experts, Cybersecurity and ICT experts from :



To identify cyber threats on Air Navigation Services in Africa



To assess current cyber resilience of Air Navigation Services in AFI region



To develop a cyber safety and resilience framework for Air Navigation Services



Benin



Kenya



Côte d'Ivoire*



Madagascar
(new)



Cameroon
(new)



Nigeria



Gambia



Somalia



Ghana



South Africa



2. DISCUSSION

2.1 Scope

2.2 Actions undertaken *(project key achievements)*

2.3 Challenges

2.4 The way Forward *(Project Upcoming Tasks and Milestones)*

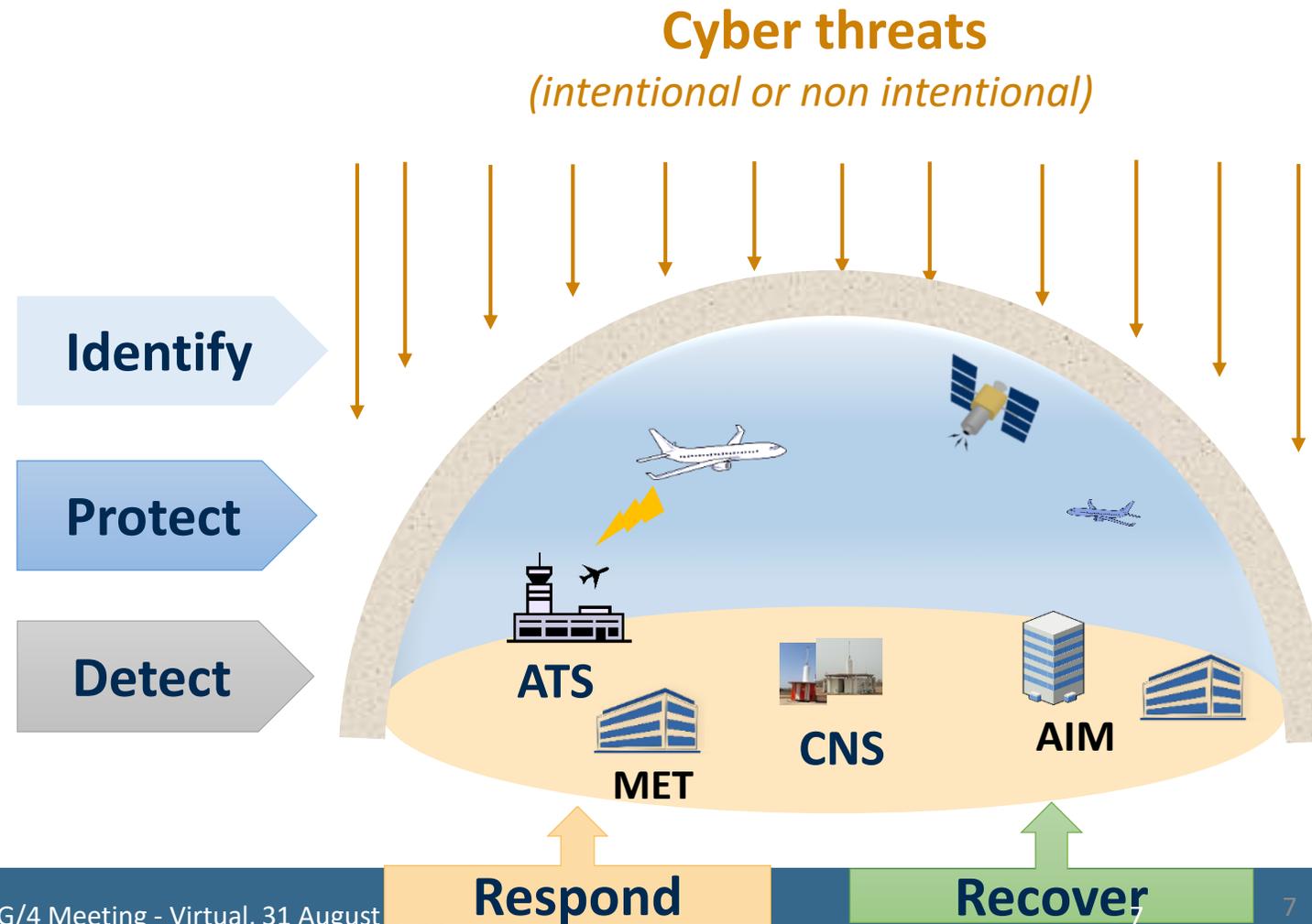


Cyber resilience

- an organisation ability to continuously deliver the intended outcome despite adverse cyber events.
- Is a measure of how well an organization can operate its business during a data breach or cyber attack



How can ANS be resilient to cyber threat?





2.2 Actions undertaken *(Project phases)*



1. Project Scope, Terms of Reference, ✓
2. Project Description, organization ✓
3. Project linkages with other IIM and AAO Projects (to be finalized)
4. Project cost estimation (to be developed)

1. Project baseline questionnaire ✓
2. Potential Cyber threats to ANS ✓
3. Analysis of feedbacks from AFI States to the questionnaires

1. Initial Analysis of existing cybersecurity and cyber resilience frameworks and guidelines (ISO 27000 series, NIST framework, ICAO thrust framework, Aviation Cybersecurity Strategy) ✓
2. Quarterly review of references documents and ongoing initiatives

1. Development and submission to IIM SG of a first edition (February 2020) ✓
2. Update of the framework
3. Submission to APIRG Review and validation

1. Promotion of the framework
2. AFI ANS Cyber resilience communication plan to raise awareness
3. Seminars/webinars on cyber resilience: awareness, training, cyber attacks simulation

1

Assess ANS Cyber resilience in AFI region

1

Identification of Potential threats to ANS

*2021 Update
AFI Region*

2

Project baseline questionnaire

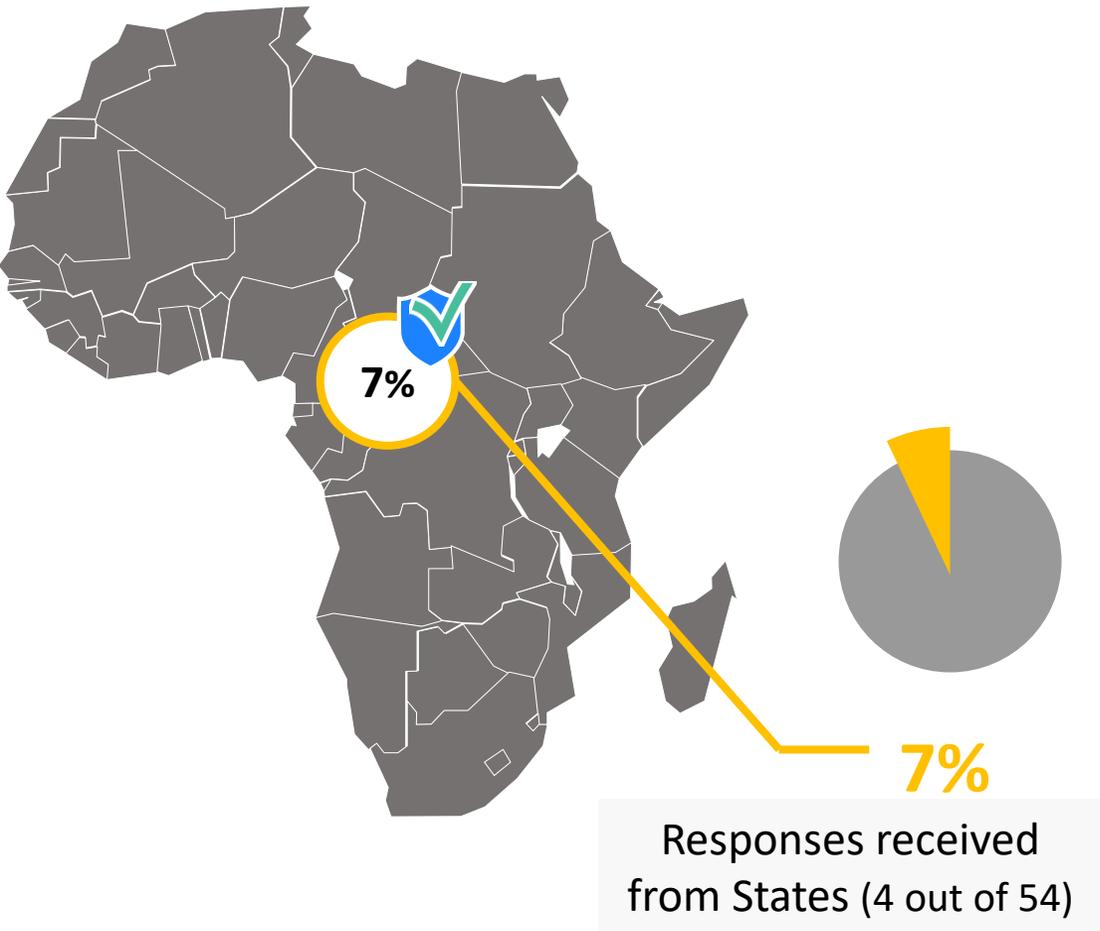
To assess current cyber resilience strategies put in place (developed and sent to AFI States)
14 questions addressing key cyber resilience aspects

3

Analysis of the responses to the questionnaires

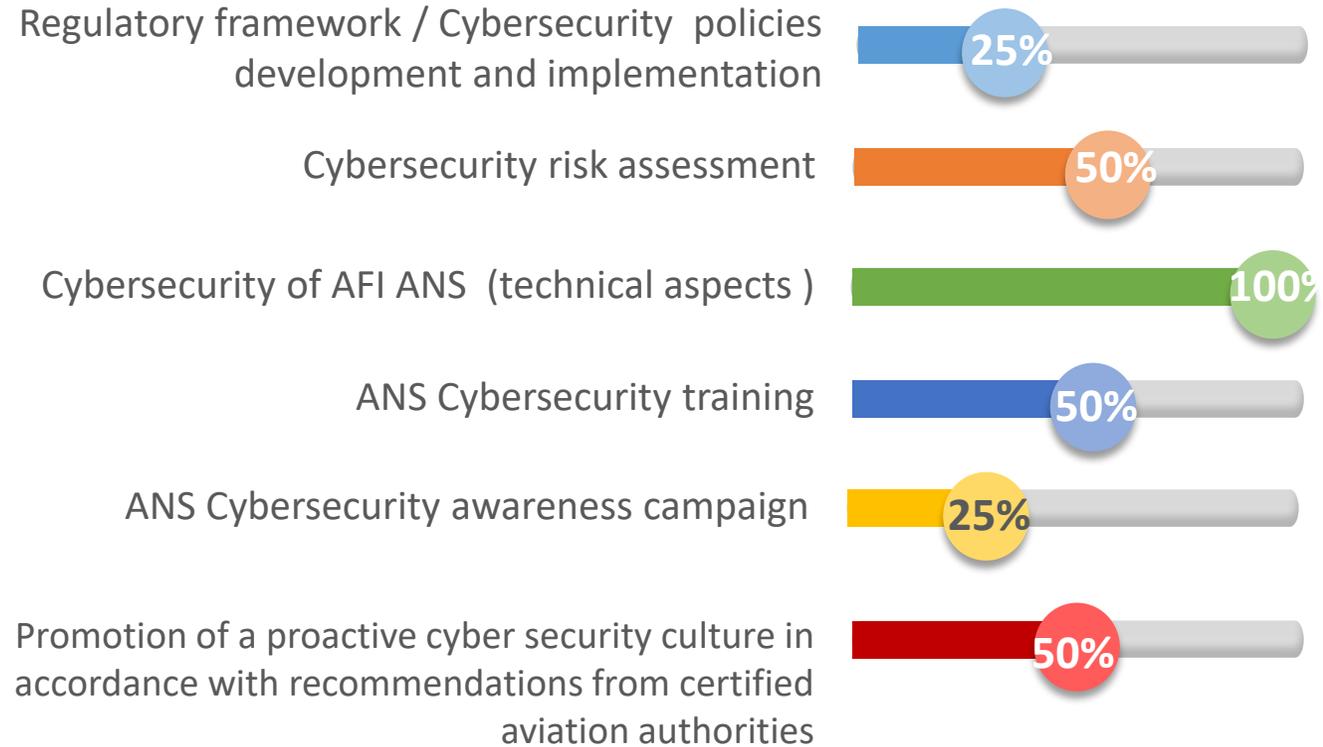
Few answers received

1 ANS Cyber resilience in AFI region Assessment



Cyber resilience key aspects to assess for AFI Region

Why States and ANSPs should respond to the IIM COM 5 questionnaire (14 questions)?



2 AFI ANS Cyber safety resilience Framework



**APIRG
INFRASTRUCTURE & INFORMATION (IIM) SUB-GROUP
COMMUNICATION PROJECT 5**

AFI Air Navigation Services Cyber Resilience Framework

| Document information | |
|--|--|
| APIRG <u>Sub Group</u> | Infrastructure & Information Management <u>APIRG Sub Group</u> |
| Project Title | Assessment of AFI Air Navigation Services Cyber Resilience |
| Project Number | IIM SG COM N°5 |
| Project Coordinator | Côte d'Ivoire |
| Deliverable Name | AFI Air Navigation Services Cyber Resilience Framework |
| Deliverable ID | D07 |
| Edition | 00.01.04 |
| Task contributors | |
| ASECNA, Benin, Côte d'Ivoire, Gambia, Ghana, IATA, Kenya, Nigeria, South Africa, Somalia | |



Provides **guidelines** that **AFI states and organizations can adopt to assess the cybersecurity risks, threats and vulnerability to the ANS systems and operations, methods of risk mitigating** , on a voluntary basis.



Identifies the main cyber threats and lists **AFI ANS Critical systems**.



Provides a **high-level guidelines and practices on cyber resilience rather than detailed technical specifications**



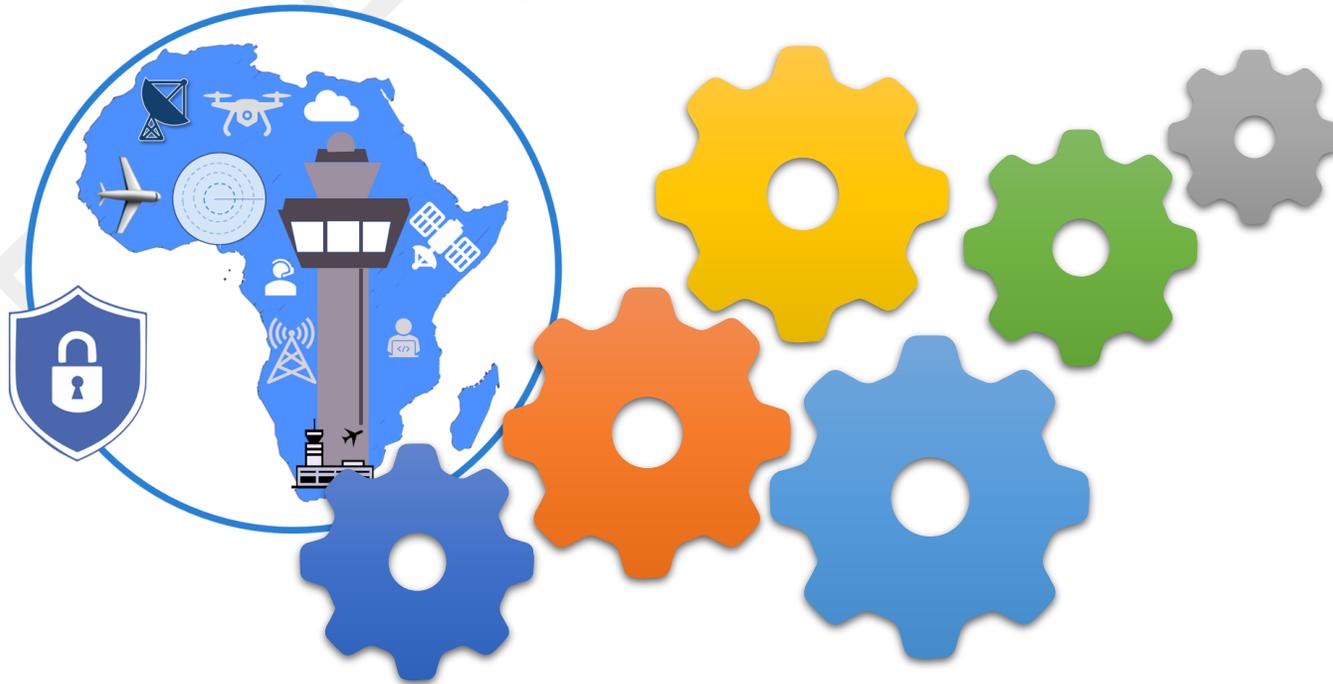
2

AFI ANS Cyber safety resilience Framework

2021 Update

INFRASTRUCTURE & INFORMATION (IIM) SUB-GROUP
COMMUNICATION PROJECT 5

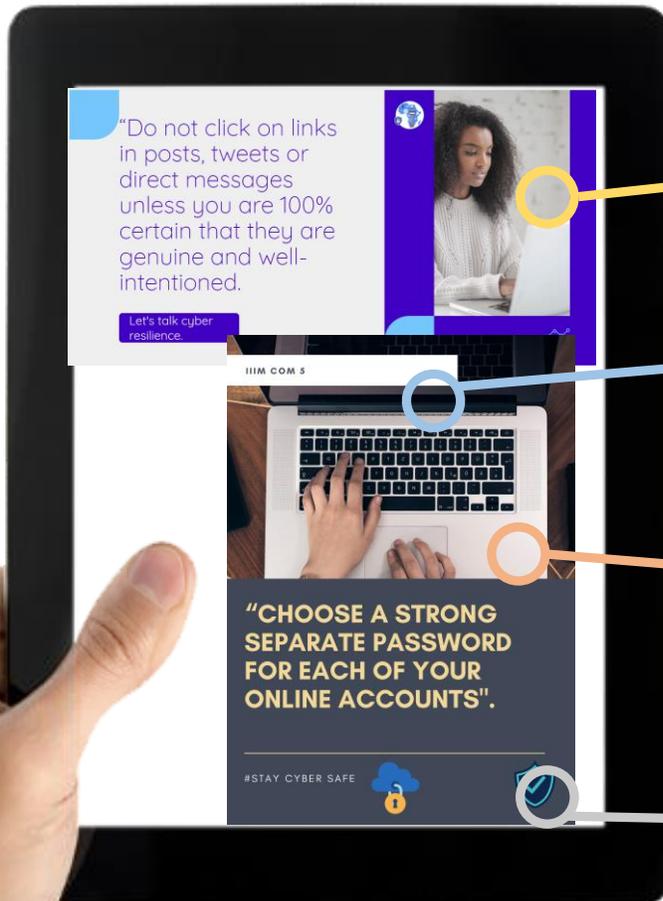
AFI Region Air Navigation Services Cyber Safety and
Resilience Framework
Edition 00.01.04



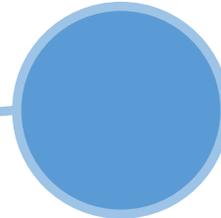
- ICAO Cybersecurity strategy (7 pillars)
- ICAO cybersecurity action plan
- CANSO guidance material (*Standard of excellence in Cybersecurity, Air Traffic Management Cybersecurity Policy Template*)
- IATA guidance material and information (Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation)
- Best practices of AFI States and other regional initiatives (EUR, NACC)
- latest input/information from ICAO Working Group on Air Navigation Systems (WG-ANS) of the ICAO SSGC

3

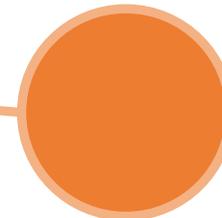
AFI ANS communication plan for cyber safety and cyber resilience awareness



A communication plan to raise awareness on cyber safety and resilience is being developed by the team



Proposition of Short messages on cyber resilience and Flyers



Promotion of key resources (documentation, training)

See example of IATA compilation of Cybersecurity Regulations Standards and guidance Applicable to Civil Aviation



Preparation of the 2021 Cybersecurity Awareness Month - observed almost globally in October

theme for 2021 'Do Your Part. #BeCyberSmart'
Seminar to be organized in October 2021

2.3 Challenges and Solutions

Challenge : few experts involved , overbooked



Experts' availability

Solution : tasks assigned on a voluntary basis.

Challenge : same experts involved in different IIM SG projects and several meetings scheduled at the same time



conflictual planning of meetings of different projects

Solution : _

Challenge : Lack of availability of the PTC



Project coordinator's availability

Solution : Appointment of Secretary and Deputy PTCs (no volunteer yet)



Challenge : Few responses to the questionnaire



Solution : Send a reminder to states with the rationale

Challenge : the list of AAO projects was needed to finalize the project linkage



Solution : list of AAO projects to be confirmed following a meeting between IIM and AAO Secretariats

Challenge : Difficulties to develop the project cost estimation

Solution : the Secretariat provided guidelines to all IIM SG Project Team Coordinators

IIM COM 5 2021-2022 objective : **let's be concrete and efficient**

Goal 1: “Make things more concrete”

- a) build concrete cyber-attacks scenarios with assistance of industry
- b) provide real examples of cyber-attacks

Goal 1: Make things more concrete Cont'd

- c) conduct seminars or webinars

Goal 2 : Finalize the core project activities” by November 2021

- a) Update of the Framework with the latest developments

Goal 2 : Finalize the core project activities” by November 2021 Cont'd

- b) Analysis of the responses to the questionnaire, c) finalize project cost estimation and project linkage

Goal 3 : “Communicate on ANS Cyber resilience (to raise awareness)” by October 2021

Three main
Result-oriented
goals for the next
period

3.1 The meeting is invited to:

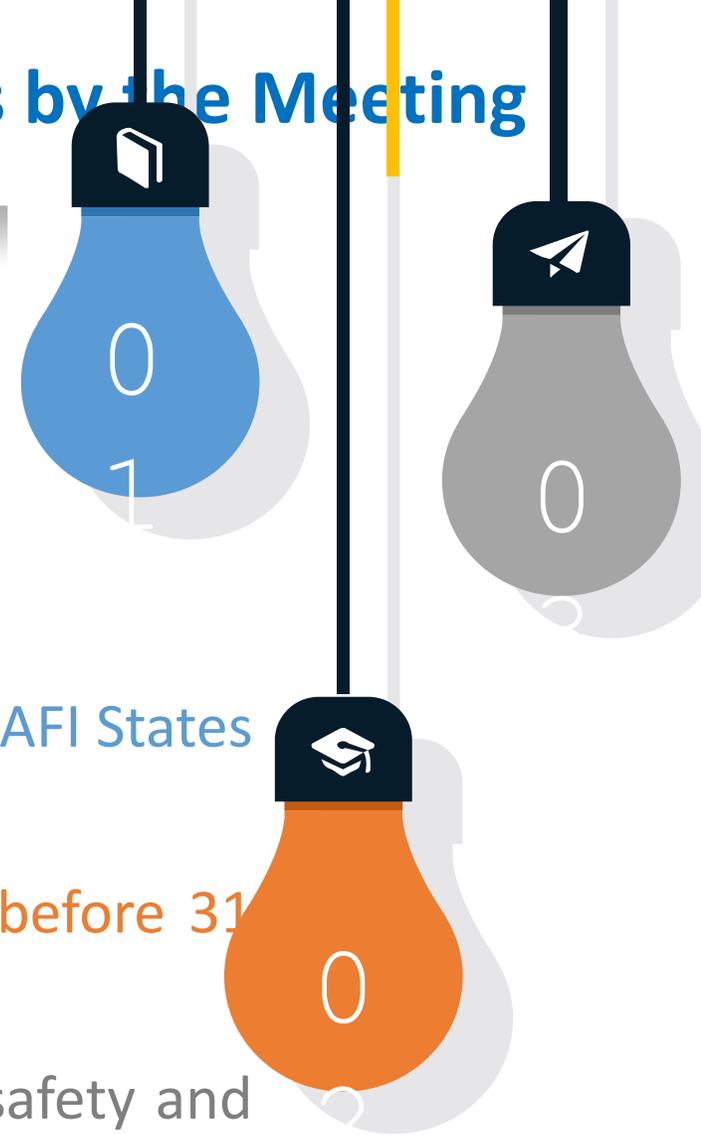
- a) Take note of the progress made so far by the project team and the challenges.
- b) Encourage State participation in the AFI region projects;
- c) Support concrete actions already taken or underway by States and organizations to respond to cyber-attacks targeting computer systems that support ATM, andand
- d) Encourage State to respond to the project Questionnaire



3.2 Draft Conclusion/Decision : Effective support to the IIM Projects activities

That;

- 1) Secretariat to distribute again the project questionnaires to AFI States and organizations
- 2) Encourage States to respond to the questionnaires on or before 31 October 2021.
- 3) APIRG support activities to raise awareness of ANS Cyber safety and resilience (*through webinars/workshops/seminars on Cyber safety and resilience for AFI Region*).





ICAO

UNITING AVIATION



<https://www.icao.int/ESAF/Pages/IIM-SG-questionnaires.aspx>



ICAO

North American
Central American
and Caribbean
(NACC) Office
Mexico City

South American
(SAM) Office
Lima

ICAO
Headquarters
Montréal

Western and
Central African
(WACAF) Office
Dakar

European and
North Atlantic
(EUR/NAT) Office
Paris

Middle East
(MID) Office
Cairo

Eastern and
Southern African
(ESAF) Office
Nairobi

Asia and Pacific
(APAC) Sub-office
Beijing

Asia and Pacific
(APAC) Office
Bangkok



THANK YOU