



SAFE SKIES.  
**SUSTAINABLE  
FUTURE.**



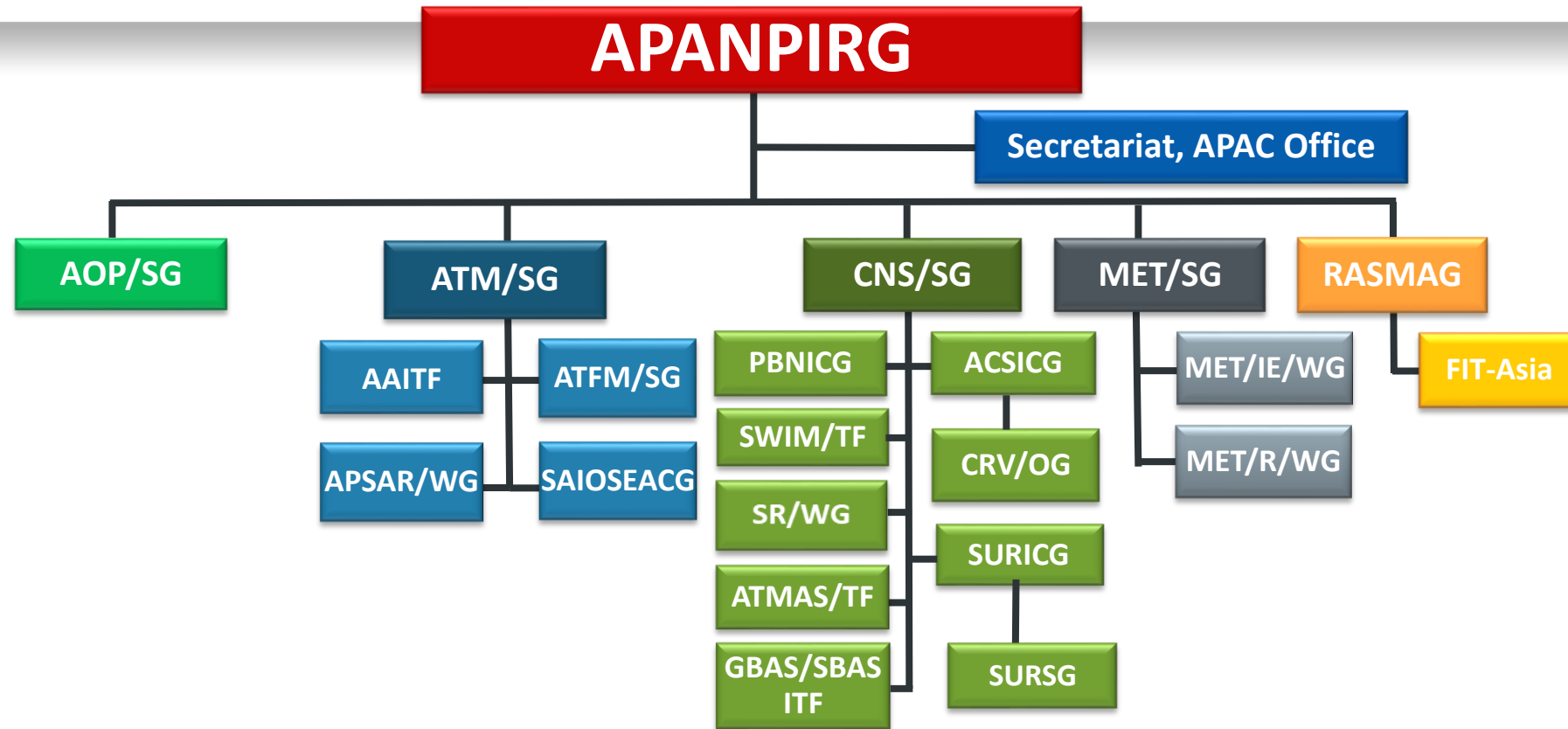
| ICAO



# Regional Perspective and Activities

Soniya Nibhani

Regional Officer, ANS (CNS) Implementation



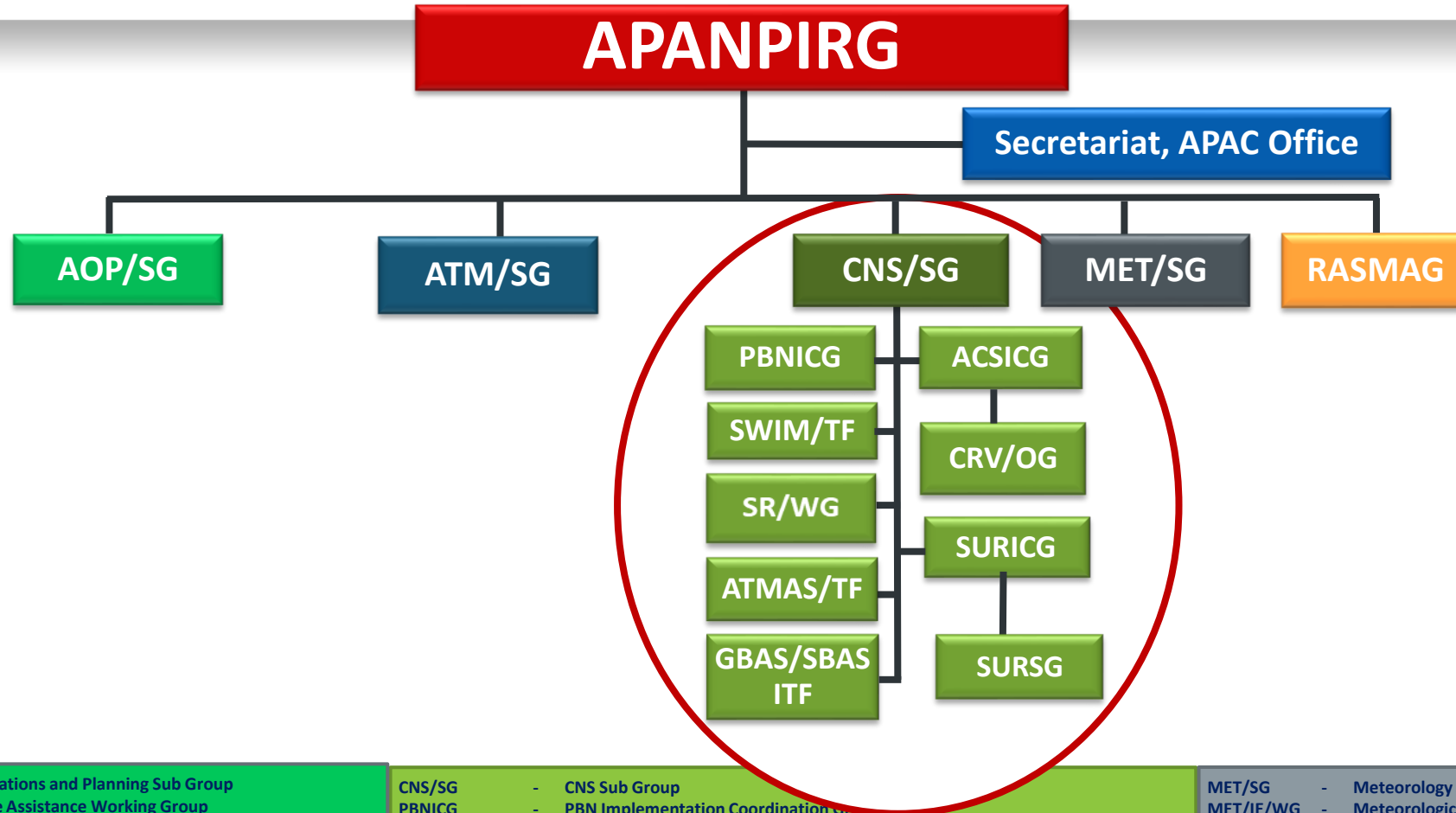
AOP/SG - Aerodrome Operations and Planning Sub Group  
 AP-AA/WG - APAC Aerodrome Assistance Working Group  
 AP-ADO/TF - APAC Aerodrome Design and Operations Task Force  
 AP-WHM/WG - APAC Wildlife Hazard Management Working Group

ATM/SG - ATM Sub Group  
 AAITF - AIS - AIM Implementation Task Force  
 APSAR/WG - APAC Search and Rescue Working Group  
 ATFM/SG - ATFM Steering Group  
 SAIOSEACG - South Asia Indian Ocean and South East Asia ATM Coordination Group

CNS/SG - CNS Sub Group  
 PBNICG - PBN Implementation Coordination Group  
 SWIM/TF - System-Wide Information Management Task Force  
 SR/WG - Spectrum Review Working Group  
 ATMAS/TF - ATM Automation System Task Force  
 GBAS/SBAS ITF - GBAS/SBAS Implementation Task Force  
 ACSICG - Aeronautical Communication Services Implementation Coordination Group  
 • CRV/OG - Common Regional Virtual Private Network (VPN) Operations Group  
 SURICG - Surveillance Implementation Coordination Group  
 • SURSG - Surveillance Study Group

MET/SG - Meteorology Sub Group  
 MET/IE/WG - Meteorological Information Exchange Working Group  
 MET/R/WG - Meteorological Requirements Working Group

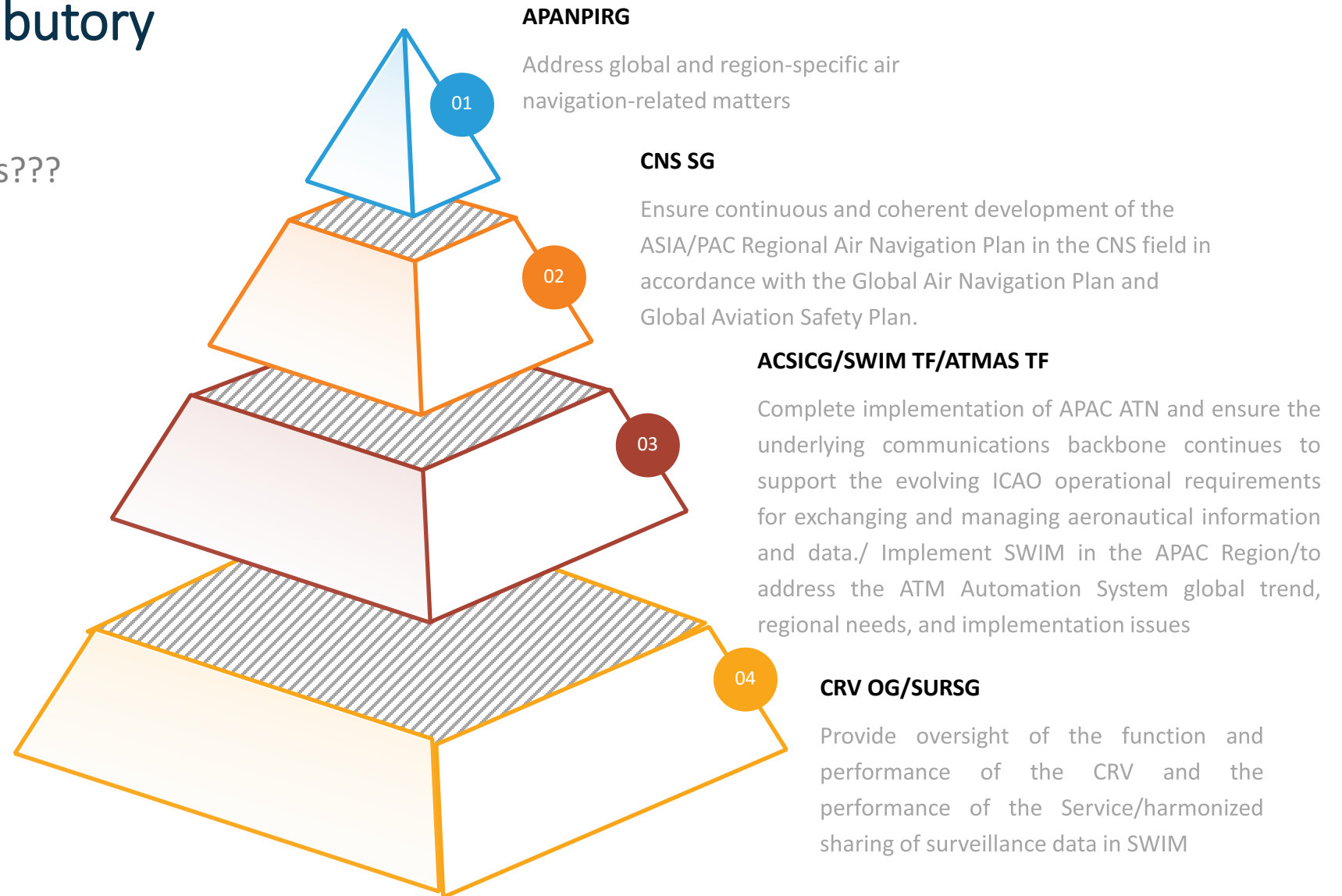
RASMAG - Regional Airspace Safety Monitoring Advisory Group  
 • FIT-ASIA - FANS Interoperability Team-Asia



AOP/SG	- Aerodrome Operations and Planning Sub Group	CNS/SG	- CNS Sub Group	MET/SG	- Meteorology Sub Group
AP-AA/WG	- APAC Aerodrome Assistance Working Group	PBNICG	- PBN Implementation Coordination Group	MET/IE/WG	- Meteorological Information Exchange Working Group
AP-ADO/TF	- APAC Aerodrome Design and Operations Task Force	SWIM/TF	- System-Wide Information Management Task Force	MET/R/WG	- Meteorological Requirements Working Group
AP-WHM/WG	- APAC Wildlife Hazard Management Working Group	SR/WG	- Spectrum Review Working Group		
		ATMAS/TF	- ATM Automation System Task Force		
ATM/SG	- ATM Sub Group	GBAS/SBAS ITF	- GBAS/SBAS Implementation Task Force	RASMAG	- Regional Airspace Safety Monitoring Advisory Group
AAITF	- AIS - AIM Implementation Task Force	ACSICG	- Aeronautical Communication Services Implementation Coordination Group	• FIT-ASIA	- FANS Interoperability Team-Asia
APSAR/WG	- APAC Search and Rescue Working Group	• CRV/OG	- Common Regional Virtual Private Network (VPN) Operations Group		
ATFM/SG	- ATFM Steering Group	SURICG	- Surveillance Implementation Coordination Group		
SAIOSEACG	- South Asia Indian Ocean and South East Asia ATM Coordination Group	• SURSG	- Surveillance Study Group		

# Key CNS Contributory bodies

Cybersecurity matters???



## Previous Cybersecurity related events/discussions

---

### **ASIA PACIFIC REGIONAL CYBERSECURITY SYMPOSIUM (APAC RCS)**

15 – 16 May 2018  
(Hong Kong China)

### **APAC CYBERSAFETY AND RESILIENCE WORKSHOP WITH TABLETOP EXERCISE (APAC TTX) (APAC CRW)**

19 – 21 November 2019  
(Bangkok, Thailand)

### **ASIA PACIFIC REGIONAL CYBERSECURITY WEBINAR**

Video Tele-Conference (VTC)  
*14 June 2021*



## ICAO ASIA/PACIFIC REGIONAL CYBERSECURITY SYMPOSIUM 2018

**Cybersecurity in Air Navigation and Airport Services**



- Held at the Civil Aviation Department Headquarters, Hong Kong China, from 15 to 16 May 2018.
- Sessions:
  - Understanding Cyber Threats and Safety Risks
  - Cyber Threats and Risks to Air Traffic Management
  - Challenges to Smart Airports in a Cyber Environment
  - Cybersecurity in User' Environment
  - How to Reduce The Threat Surface
  - Cyber Safety and Resilience

## ASIA PACIFIC REGIONAL CYBERSECURITY WEBINAR

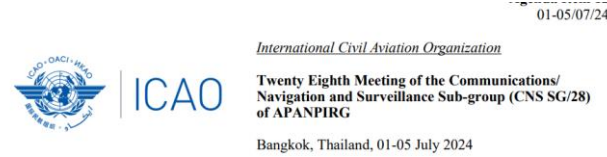
- Held by VTC on 14 June 2021.
- Sessions:
  - ICAO Trust Framework Latest Development
  - FAA's contribution to the IATF and the Importance of IATF to FAA
  - Cyber Safety in ATM
  - Protecting All Systems
  - DNS Ecosystem Security
  - Building Mutual Trust Infrastructure Based on Block Chain
  - A proactive and systematic approach in protecting digitized air traffic services against cyber threats in Hong Kong
  - Air Traffic Management Security and Updates on ICAO Cybersecurity Activities
  - A Security Solution for Information Services in SWIM
  - Cybersecurity – A vendor's perspective



## APAC CYBERSAFETY AND RESILIENCE WORKSHOP WITH TABLETOP EXERCISE (APAC TTX)

- 19 – 21 November 2019 at ICAO APAC Office, Bangkok, Thailand.
- Three scenarios:
  - Discussions on Scenario 1 – Future airlines is missing flight plan acknowledgements from enroute ANSPs. Future Airlines keeps submitting the flight plans till they get an acknowledgement. Flooding/Duplicated Flight Plans into the FPL processing (FDP) and also surveillance data sharing
  - Discussions on Scenario 2 – The media is aware of the issue going on. ANSP leadership tries to coordinate a common response. The issues within the ATM infrastructure have undermined the capacity of the system by 50%
  - Discussions on Scenario 3 - Capital City Airport (Flight Information Display Sub-System- FIDS malfunction)

# Previous Cybersecurity related events/discussions



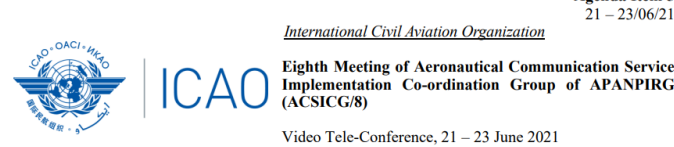
- Agenda Item 12:** Cybersecurity of CNS/ATM systems  
12.2 Other Cybersecurity related matters

## STRENGTHENING AVIATION CYBERSECURITY THROUGH ORGANIZING ATTACK-WITH-DEFENCE EXERCISE

(Presented by Hong Kong, China)

### SUMMARY

In the ever-changing landscape in aviation cybersecurity, traditional training may not provide cybersecurity personnel with real-world experience in handling actual cyber-attacks. Organizing an Attack-with-Defence exercise under simulated and controlled environment is beneficial in strengthening cybersecurity personnel's understanding on attacker's mindset and skills, while enhancing awareness and preparedness to respond to cyber-attacks.



- Agenda Item 5:** Review and update the AMHS/ATN Implementation Status

## IMPLICATIONS OF CYBERSECURITY AND ASSOCIATED REQUIREMENTS FOR CRV OPERATIONS

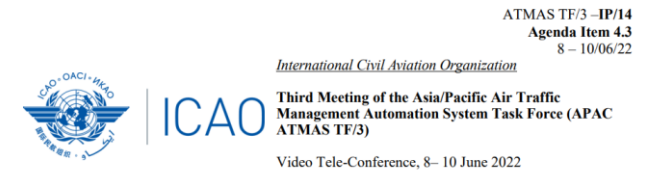
(Presented by United States / FAA)

### SUMMARY

This flimsy reviews the current and envisioned future environments for CRV operations to provide a framework for discussion of requirements for Cyber Security and SWIM.

## 1. INTRODUCTION

1.1 This flimsy addresses the implications for existing services and the Asia Pacific Common AeRonautical Virtual Private Network (CRV) resulting from the recent Cybersecurity Webinar<sup>1</sup> and future support of SWIM and other proposed services for the Region.



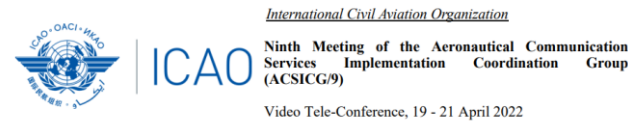
- Agenda Item 4:** ATM Automation System Implementation by States  
4.3 Development of New Technology

## ATMAS CYBERSECURITY DESIGN IN BRIEF

(Presented by China)

### SUMMARY

This paper presents the current cybersecurity status of Air Traffic Management Automation System (ATMAS) in China, and the brief design on 3 key aspects of cybersecurity in common between ICAO Doc 9985 and Chinese cyber security standard serial (GB/T 22239-2019).



- Agenda Item 8:** Issues on AFS related cyber-safety/security and resilience

## AERONAUTICAL FIXED SERVICE (AFS) CYBERSECURITY CONSIDERATIONS FOR INFORMATION OVER CRV

(Presented by United States / FAA)

### SUMMARY

This paper presents some security considerations for CRV data exchanges in the light of increased Cyber Threat because of World events.

## 1. INTRODUCTION

1.1 The 2021 Regional Cybersecurity Webinar<sup>1</sup> presented the work of the International Aviation Trust Framework (IATF) initiative. The IATF is composed of Digital Identity and Network Information Security elements. At the Twenty Fifth Meeting of the Communications Navigation and

# Previous Cybersecurity related events/discussions

## 3. SUGGESTED IMPLICATIONS

3.1 The meeting is invited to comment and discuss these suggested implications:

### 3.1.1 ICAO Requirements

- a) ICAO needs to provide an IPv6 dedicated address block
- b) ICAO needs to propose a Name Space and field DNS
- c) ICAO needs to provide the Trust Framework for Digital Identities

### 3.1.2 CRV Network Requirements

- d) CRV needs to plan to implement IPV6
- e) CRV needs to provide transport for DNS access and distribution
- f) CRV needs to provide transport for Digital Identity access and verification

### 3.1.3 Service Provider Options

- g) Service Providers may offer optional SWIM services, or applications built on SWIM services, to Users.

### 3.1.4 CRV User Requirements

- h) CRV Users need to implement network security
- i) CRV Users need to plan to implement IPv6
- j) CRV Users need to plan to implement DNS
- k) CRV Users need to plan to adopt Digital Identities, as prescribed by ICAO, and use them in connections with SWIM services
- l) CRV Users may implement SWIM, may access SWIM as a service, or may adopt some hybrid of the two.
- m) CRV Users may implement data integrity by digital signing

# Previous Cybersecurity related events/discussions

## *Network Information Security*

2.3 Network Information Security requirements were described<sup>1</sup> as: IPv6, a Domain Name System (DNS), information security, network management and network contingencies.

2.4 The IATF envisions that the aviation community will inter-communicate using *IPv6 addresses*, from an ICAO block, so that aviation users can be identified. ICAO still has to fulfill its obligation to obtain such a block of addresses and allow the community to plan for their introduction.

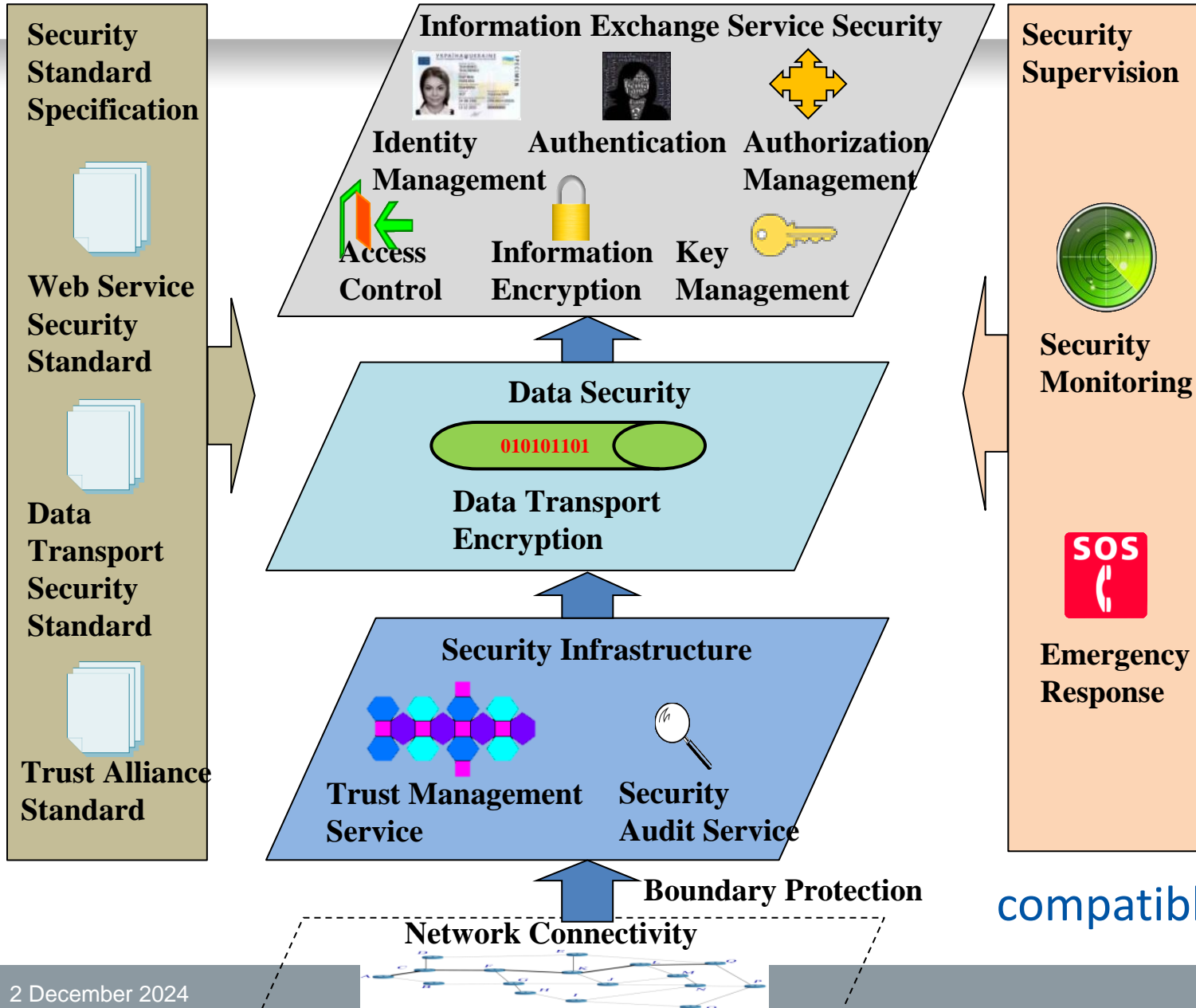
2.5 Likewise, a secure *Domain Name System* (DNS) has been discussed for more than a decade but not yet materialized. DNS is essential to fulfill the Digital Identity concept.

2.6 *Information Security* applies to both data integrity and confidentiality. As previously mentioned, PKI Certificates can play a large role in this area but in the interim existing methods must be used:

- Sensitive data can be exchanged using IPsec tunnels, and that should always be the case when exchanging data over a public network.
- Incoming information should be scanned for malicious content by an edge device or firewall. This applies to information from existing trusted correspondents who may have been unknowingly compromised.
- Weather data is starting to be exchanged using ICAO Weather Information Exchange Model (IWXXM) encoded in Extensible Markup Language (XML). As an AMHS File Transfer Body Part (FTBP), this information payload will typically be scanned as part of the AMHS message information. Additional schema validation should be performed on the IWXXM data either programmatically or with a specialized security device. This is especially important since the IWXXM data may be compressed for FTBP exchange.

# The Cybersecurity Architecture Framework of SWIM

- WP/09 - *Cyber Security Architecture Framework of SWIM*, presented under agenda 3-d SWIM Governance at APAC SWIM TF/3 held from 7 -10 May 2019 in Bangkok.
- The design principle
  - **Integration Principle**: Integrate security depth into all levels of SWIM to form endogenous security attributes.
  - **Appropriate Principle**: Consider security and efficiency, balancing security risk and security investment.
  - **Cyber Resilience**: Establish a multi-layer security protection system to deal with cyber-attacks, with disaster recovery capabilities to ensure business continuity.
  - **Principle of Equality**: Consider different policies and regulations in different countries, to ensure the sovereignty of each country in cyberspace

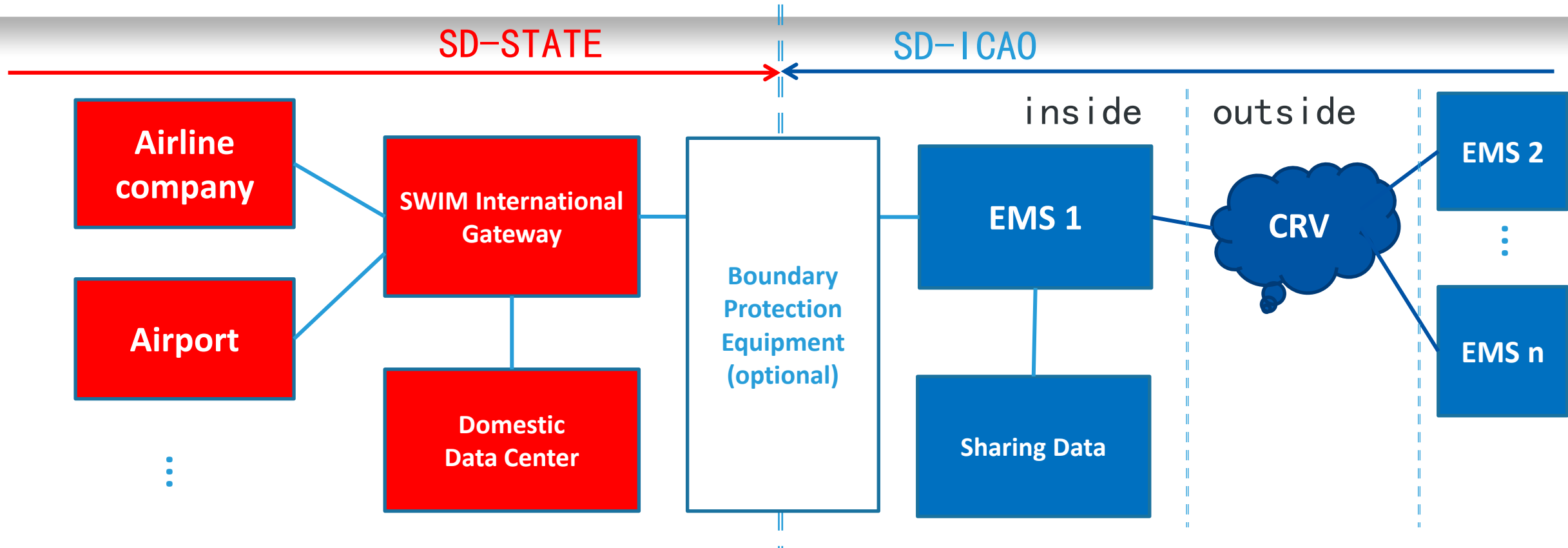


## Security Technical Architecture Framework

- **Security Infrastructure:** Provide core security services support;
- **Data Security:** Implement the security of data exchange and sharing;
- **Information Exchange Service Security:** Provide security protection for SWIM services.

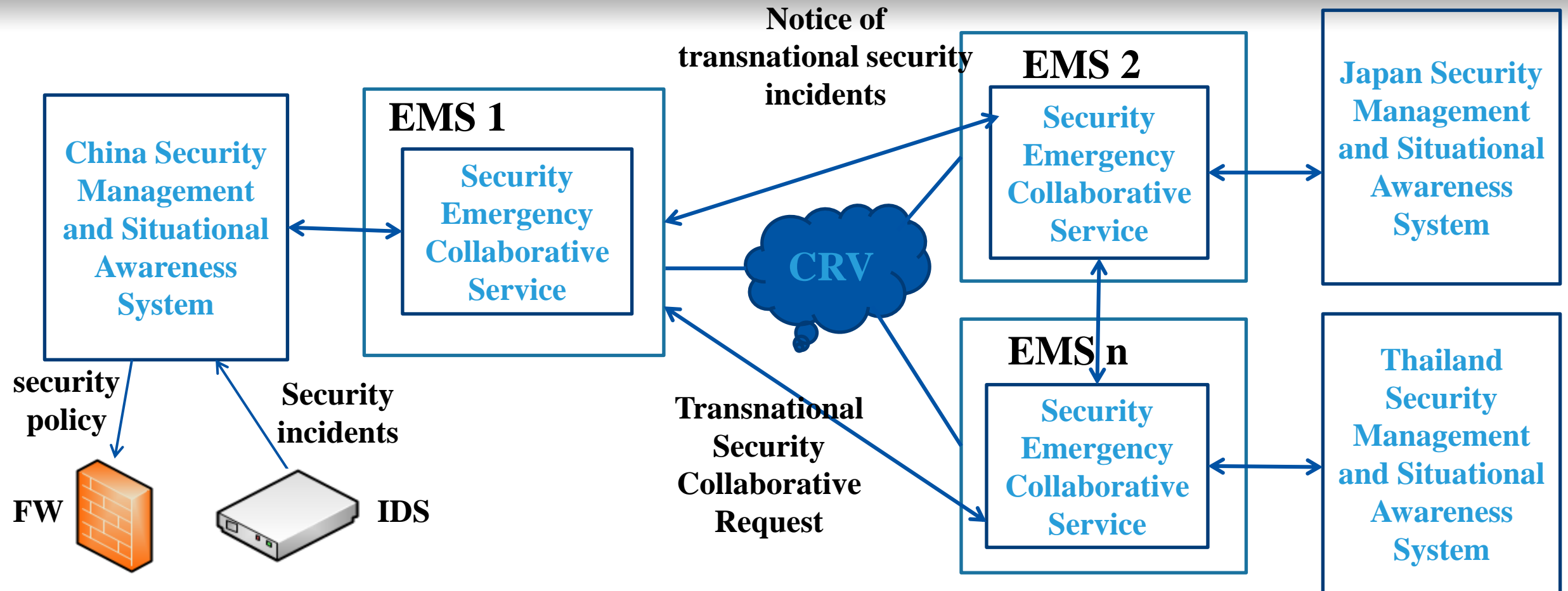
compatible with ICAO Doc10039





- Each country node has **two** security domains: the red one is the domestic Security Domain; the blue one is the ICAO Security Domain.
- Different state Security Domains can implement **different security strategy**;
- The security strategy in ICAO Security Domain are determined by consensus of the states in ICAO;
- Data in different security domains are stored in different zones.

## Example: Emergency Cooperative Response Mechanism



- **Security emergency collaborative:** provide notifications of security incidents and collaborative request.
- the source of attack can be located and the route of virus transmission can be cut off.



## Proposal to Establish a Regional WG on Cybersecurity

- The CNS SG/22 meeting held at the APAC Office in July 2018 discussed the proposal and **considered it better to wait for further guidance to be developed at the global level to avoid duplicated efforts.**
- The SWIM TF/3 meeting held in May 2019 endorsed a proposal to establish a **Task Group to look into a cyber security framework in order to progress the security element of SWIM governance.**

# Report of SWIM TF/8 and SWIM TF/9

- The Eighth Meeting of the System Wide Information Management Task Force (SWIM TF/8) - **8 to 10 November 2023**
- The Ninth Meeting of the System Wide Information Management Task Force (SWIM TF/9) - **14 to 17 May 2024**
- Both at ICAO Asia and Pacific Regional Office, Bangkok.



## Report of SWIM TF/8 and SWIM TF/9

### *Guidance on provisions of ICAO DOC 10204- Manual on Information Security*

- The SWIM TF/9 Meeting noted the need for a dedicated group to support APAC Member States/Administrations in implementing recommendations being developed by the TFP. SWIM TF/9 requested CNS SG/28 to provide guidance, especially for the group responsible for implementing information security provisions in the APAC region.

# The Twenty-Eighth Meeting of the Communications, Navigation and Surveillance Sub-group (CNS SG/28)

- 1-5 July 2024 at the ICAO APAC Regional Office, Bangkok, Thailand
- **120** participants from **25** States/Administrations, **3** International Organizations and **6** participants from industry partners.





### *Guidance on provisions of ICAO DOC 10204- Manual on Information Security*

- The CNS SG/28 Meeting deliberated the requirements to establish a dedicated group to support the implementation of the ICAO information security provisions in the APAC region. With the expectation that the *Manual on Information Security* is to be published in the second half of 2024, later than the time of the CNS SG/28, the Meeting discussed that the APAC States/Administration would need adequate time to study and understand the content and recommendations contained in the manual before making a decision on the appropriate way forwards.
- Therefore, it was advised that the discussion on forming a dedicated group be deferred to the CNS SG/29 Meeting in 2025.

## Summary

- Cybersecurity considerations:
  - ✓ Aeronautical Fixed Services
  - ✓ SWIM
  - ✓ ATM Automation system.....
- Long waiting for ICAO Provisions on:
  - ✓ IPv6 Address allocation
  - ✓ IP Network Security
  - ✓ ATM Automation System Security
  - ✓ Information Security

---

# Thank You

