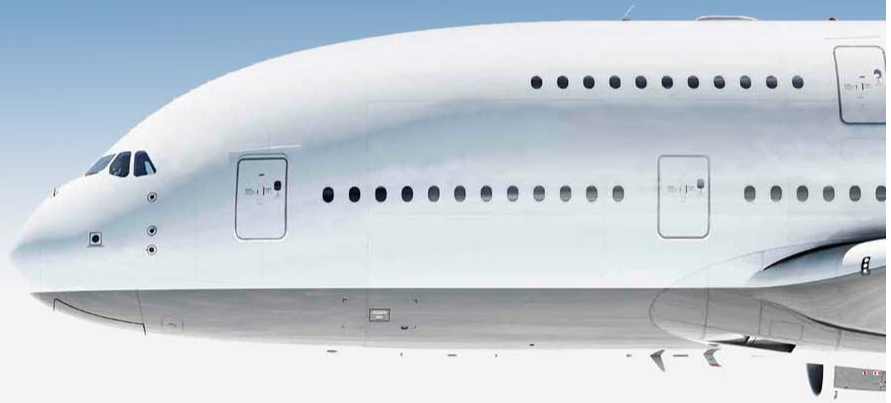
ICAO SECURITY & FACILITATION

AIR TRAFFIC MANAGEMENT SECURITY AND UPDATES ON ICAO CYBERSECURITY ACTIVITIES

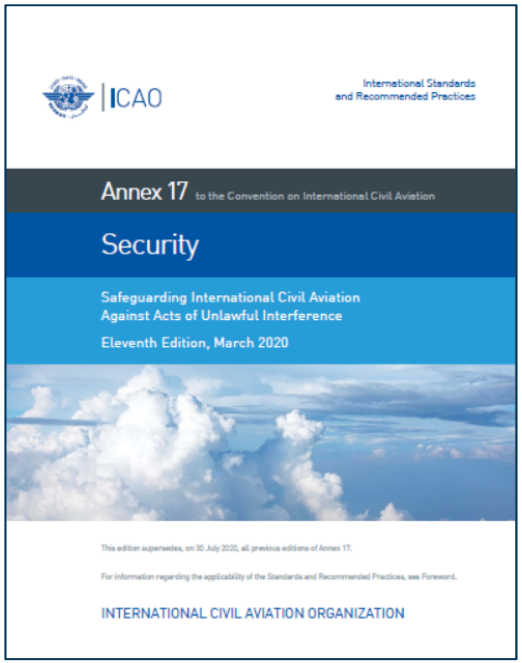


Mr. Remington Low
ICAO Regional Officer
Aviation Security & Facilitation

Annex 17 – Security (Amendment 17)

Aviation security Standards and Recommended Practices (SARPs) are mainly contained in Annex 17 - *Security*

Security provisions also in other Annexes (Annex 2, 6, 8, 9, 10, 11, 14, 18) and PANS Docs 4444 and 8168.



National Civil Aviation Security Programme

Annex 17 – *Security* requires States to develop and implement a NCASP:

- addresses the whole range of security activities including, threat and risk assessment, staff selection and training (in security-related matters), access control and other preventive security measures, management of response to AUIs

- roles and responsibilities of all agencies, including Air Traffic Services (ATS) Providers, as related to security operations

Relevant SARPs to ATS Providers

- S 3.5: require ATSP … to establish and implement appropriate security provisions to meet the requirements of the NCASP
- S 4.9.1: identify their critical information and communications technology systems and data ..in accordance with a risk assessment, develop and implement, …measures to protect them..
- RP 4.9.2: ensure …measures protect, …the confidentiality, integrity and availability of the identified critical systems and data. The measures should include …security by design, supply chain security, .., and the protection ..of any remote access capabilities, …

ICAO's Work on Cybersecurity

Legal Instruments:

- The Beijing Convention and The Beijing Protocol of 2010

Assembly Resolutions:

- A39-19 and A40-10 Resolutions on Cybersecurity

Standards and Recommended Practices:

- Annex 17 – *Security*: Standard 4.9.1 and Recommended Practice 4.9.2

Guidance Material:

- Procedures for Air Navigation Services – PANS
- Doc 8973 – *Aviation Security Manual*
- Doc 9985 – *ATM Security Manual*
- Aviation Cybersecurity Strategy
- Cybersecurity Action Plan

Training

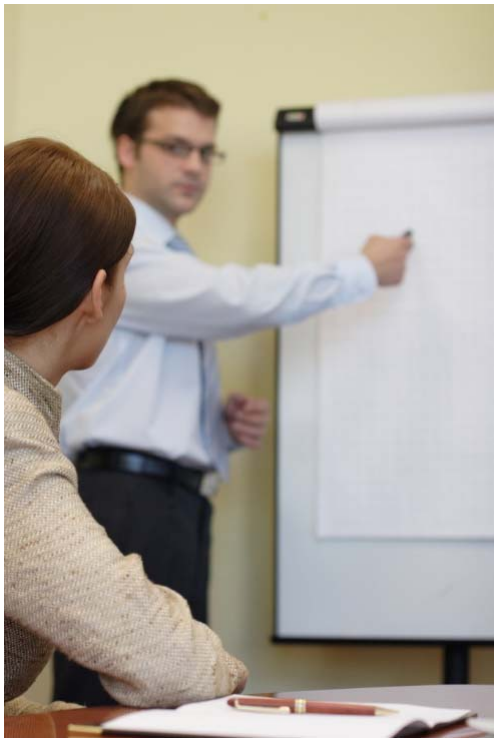
- Cybersecurity Training Roadmap
- Training Courses

ICAO Guidance Materials

- Air Traffic Management Security Manual (Doc 9985, Restricted)
- PANS
- Aviation Security Manual (Doc 8973, Restricted – 12th edition)
- ICAO global Risk Context Statement (Doc 10108, Restricted – 2nd edition)
- Aviation Cybersecurity Strategy
- Cybersecurity Action Plan

Training

- **Training Courses in the Pipeline:**
  - ✓ Foundations of Aviation cybersecurity Leadership and Technical Management
    - Developed in Partnership between ICAO and Embry-Riddle Aeronautical University
    - Two Tracks: Leadership & Technical Management
  - ✓ Managing Security in ATM
    - Developed in Partnership between ICAO and EuroControl
    - Covers Traditional ATM Security as well as Cyber

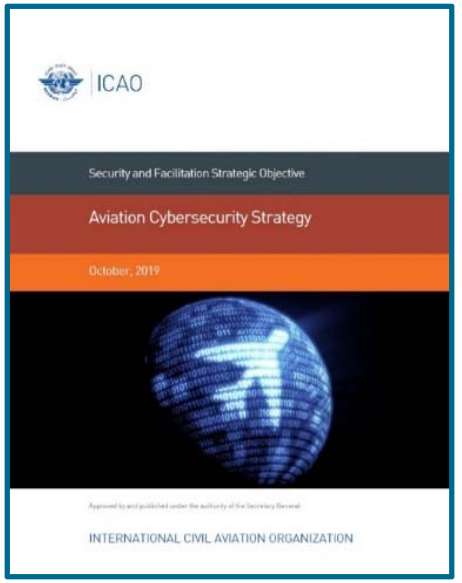


Expert Groups within ICAO Addressing Cybersecurity in their Work

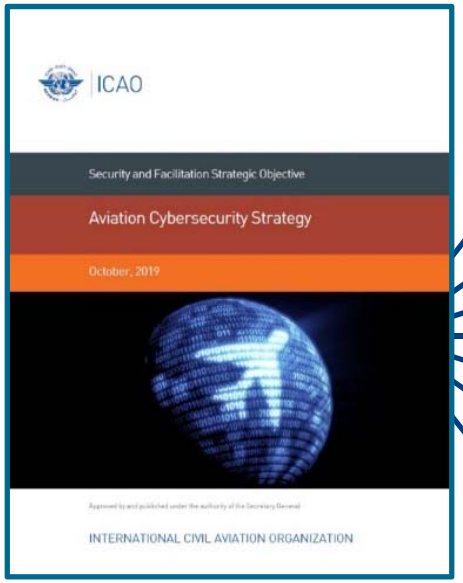
- **Secretariat Study Group on Cybersecurity – SSGC (late 2017)**
  - ✓ Research Sub-Group on Legal Aspects
  - ✓ Working Group on Airline and Aerodromes
  - ✓ Working Group on Air Navigation Systems
  - ✓ Working Group on Cybersecurity for Flight Safety
- **Trust Framework Study Group – TFSG**
  - ✓ Trust Reciprocity Operational Needs Working Group
  - ✓ Digital Identity Working Group
  - ✓ Global Resilient Aviation Interoperable Network Working Group

Aviation Cybersecurity Strategy

- To protect and ensure continuity of civil aviation operations from cybersecurity threats that affect the safety, security and trust of the air transport system;
- To have 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
- To allow coordination of cybersecurity measures among State to ensure effective and efficient management of cybersecurity risks.



Aviation Cybersecurity Strategy



- International Cooperation
- Governance
- Effective Legislation & Regulations
- Cybersecurity Policy
- Information Sharing
- Incident Management & Emergency Planning
- Capacity Building, Training, & Cybersecurity Culture

Cybersecurity Action Plan

- 1st edition published in November 2020 issued via State letter 2020/114.
- **Provides the Foundation** for ICAO, States and stakeholders to work together, and proposes a **Series of Principles, Measures, and Actions** to achieve the objectives of the Cybersecurity Strategy's seven pillars.
- **Develops the Seven Pillars** of the Aviation Cybersecurity Strategy into **29 Priority Actions**, which are further broken down into **54 Tasks** to be Implemented by ICAO, States, and Stakeholders

Cybersecurity Action Plan (Example)

Priority Outcome	Pillar 3: DEVELOP EFFECTIVE LEGISLATION AND REGULATIONS
Priority Actions	• Ensure that appropriate regulation and legislation are in place for cybersecurity; • Develop appropriate guidelines for States and Industry in implementing cybersecurity related provisions; • Ensure that international legal instruments provide appropriate measure for the prevention, timely reaction to, and prosecution of cyber-incidents.

Actions

Action #	By	Traceability to the Cybersecurity Strategy	Traceability in Action Plan	Specific Measures/Tasks	Indicators	Maturity	Target
CyAP 3.1	Member States	3.3	8.4	Member States to ratify Beijing instruments.	Number of States having ratified Beijing instruments	Low	ongoing
CyAP 3.2	ICAO	3.3	8.3	Analysis of international air law instruments	Report and update plan	N/A	2020
CyAP 3.3	ICAO and Member States	3.3	8.2	Analysis of existing international and national legislation in the cybersecurity field and identify gaps, including criminal law.	Promote ratification of instruments to incriminate unlawful cyber acts.	Medium	2022 - 2023
CyAP 3.4	ICAO, Member States and Industry	3.3	8.1	Review existing ICAO security standards to identify need for potential cybersecurity updates	Regulatory gap analysis	High	2021
CyAP 3.5	ICAO	3.2	5.4	Create, review and amend guidance material related to implementing cybersecurity requirements	Accepted and agreed cybersecurity guidance material	High	2021-2022

ICAO SECURITY & FACILITATION

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