

# CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION  
FROM CYBER ATTACKS

DOHA, QATAR | 6 - 8 NOVEMBER 2023



ICAO MID



## Cybersecurity Governance in Civil Aviation: Oman's Experience

Saif AL Ghafri, Cyber Security Inspector

## Objective

- ✈ Showcasing The Experience Of The Sultanate Of Oman In Cybersecurity Governance In Civil Aviation

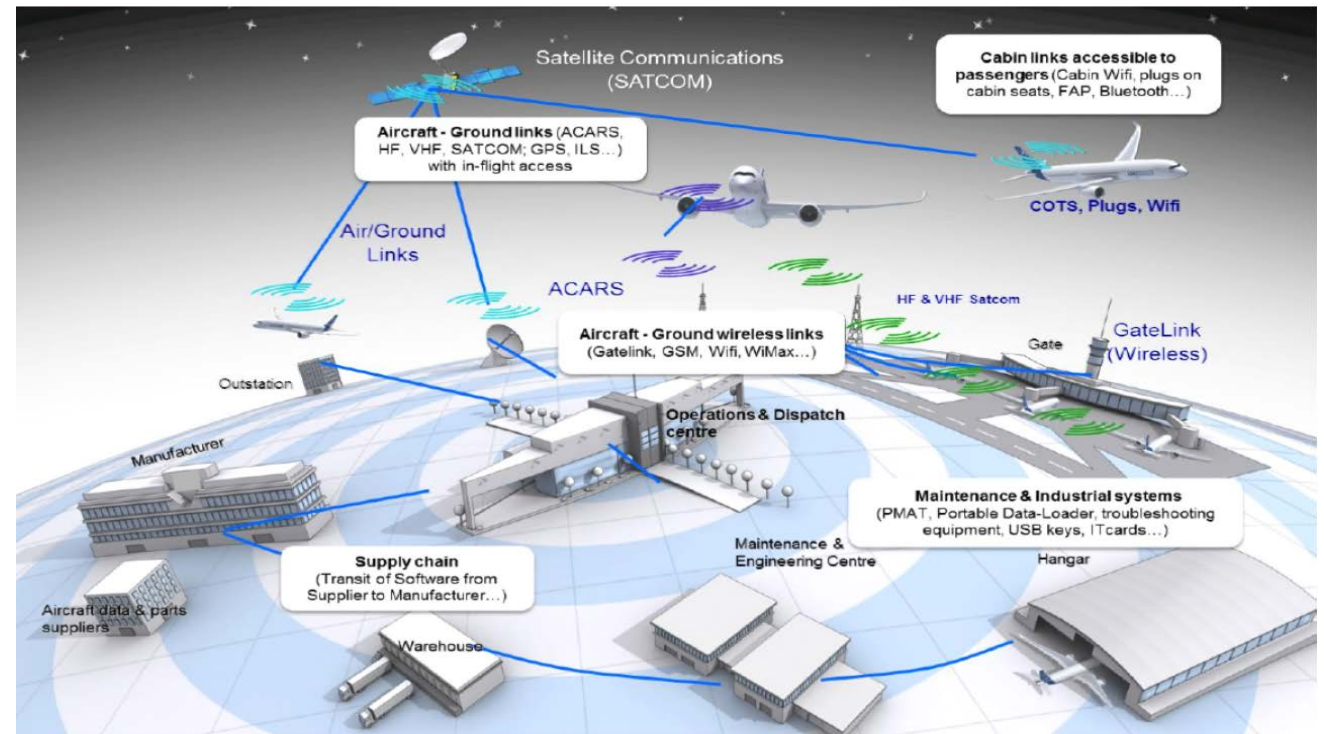
نتقدم بثقة  
Moving Forward  
with Confidence

رؤية عُمان  
2040  
OmanVision



# Interconnection of Networks

✈ The network in civil aviation sector is interconnected with all operational entities, including security and other relevant government entities. The networks are also interconnected internationally in aspects related to operations for sending and receiving relevant information.



# Annex 17 to the Chicago Convention - Security

## ✈ **Standard 4.9.1**

Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.

## ✈ **Recommended Practice 4.9.2**

Recommendation— Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities.

## The National Level

### ✈ The Responsibility

Regulating cybersecurity has been assigned to the Aviation Security and Facilities Department at the Civil Aviation Authority, whereby the Aviation Security Regulation Section is responsible for preparing and updating regulations, the Quality Control and Licensing Section is implementing quality control activities, and the Risk Assessment Section is working on assessing cybersecurity risks.



# The Operational Level

## ✈ The Responsibility

Operational entities are responsible for adhering to national requirements, developing standard operating procedures, and implementing the necessary procedures to protect critical information and communications technology systems and data used for civil aviation purposes.



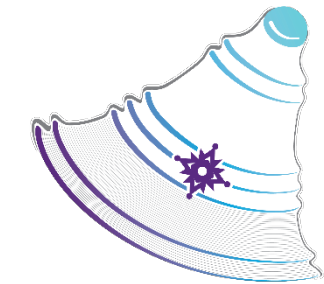
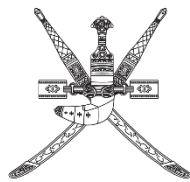
## Sources for Developing Cybersecurity Regulations and Procedures

- ✈ **Annex 17**  
Standard 4.9.1, Recommended Practice 4.9.2
- ✈ **Aviation Security Manual**  
Doc. 8973
- ✈ **National Legislations**  
Linking civil aviation policies and regulations with international and national requirements in a way that meets the country's policy towards cybersecurity

## Coordination & Communication

- ✈ Continuous coordination between the Civil Aviation Authority and the relevant cybersecurity authorities in the Sultanate of Oman (the Cyber Defense Center and the Ministry of Transport, Communications and Information Technology) and other entities at the operational level in the sector to keep pace with the changes and developments of cybersecurity threats
- ✈ A technical committee concerned with cybersecurity has been established, emanating from the National Committee for Civil Aviation Security and Facilities

سلطنة عُمان  
وزارة النقل والاتصالات وتقنية المعلومات  
Sultanate of Oman  
Ministry of Transport, Communications and  
Information Technology



مركز الدفاع الإلكتروني  
Cyber Defense Centre





## Committee Responsibilities

- ✈ Ensuring coordination of cybersecurity measures and controls between the various departments and entities responsible for protecting the interconnected network components and systems the sector
- ✈ Continuously review and evaluate the efficiency of the sector's cybersecurity measures as threats change and provide recommendations for changes in these measures based on threat information, technology revolution, aviation security techniques, and other factors
- ✈ Implementing security assessments to examine the readiness of cybersecurity measures and precautionary measures related to the protection of private operational and commercial systems, communications devices and technologies used in the civil aviation sector in order to ensure they are protected from being penetrated

## Committee Responsibilities Cont.

- ✈ Classifying and identifying critical infrastructure and relevant entities, and identifying sectors based on priority
- ✈ Establishing frameworks and controls for responding to cybersecurity incidents, monitor compliance, and update them
- ✈ Developing cybersecurity KPI's, and preparing periodic reports on the status of cybersecurity in the sector in the Sultanate of Oman
- ✈ Notifying relevant entities of the risks of cyber threats to take corrective actions
- ✈ Ensure that relevant entities take necessary measures to mitigate the risks of cyber attacks
- ✈ Raising the level of cybersecurity awareness among employees

## Cybersecurity Awareness

- ✈ Enhancing the level of security awareness and instilling cybersecurity culture is one of the ways to prevent cyber threats. Accordingly, awareness brochures and circulars have been distributed and disseminated through various internal communication channels for relevant entities in the sector. Additionally, security awareness courses have been organized and conducted in the areas of cyber risks, threats and protection methods



## Cybersecurity Challenges

- ✈ Cyber threats and incidents are becoming costly and complex than ever
- ✈ Reliance on ICT in aviation operations and integrations with other organizations
- ✈ The high cost of implementing necessary cybersecurity requirements
- ✈ Outdated Aviation Software Systems
- ✈ Shortage of professional specialists in this field
- ✈ High salaries, as a result of the high demand for expertise in this field
- ✈ High cost of specialized training
- ✈ Increased prices of cybersecurity solutions, consultation services, security assessments, and penetration testing

## Conclusion

- ✈ The Aviation industry is vastly relying on technology
- ✈ Cybersecurity should be governed in civil aviation
- ✈ Tasks, responsibilities, and results should be communicated, monitored, and assessed
- ✈ Cybersecurity Awareness is the key to minimize cyber risks
- ✈ The best way to implement Cybersecurity Awareness is to use platforms

# CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION  
FROM CYBER ATTACKS

DOHA, QATAR | 6 - 8 NOVEMBER 2023

# THANK YOU

