Barriers to Secure Skies: The Cybersecurity Challenges of Connected Avionics

Image Source: https://www.pexels.com/photo/white-and-red-plane-beside-clouds-low-angle-photography-46148/

PRAVEEN K R

Social Profile: https://www.linkedin.com/in/praveen-k-r-0a526617/

- **20 + Years of overall Industry Experience of which**
  - 12+ in Product Security Practices
  - 8+ in Verification & Validation
- **Domains Worked for:**
  - Industrial Automation
  - Aerospace
- **Bachelors in Electronics & Communication Engineering**
- **Masters in Computer Science**
- **Cybersecurity Manager at Honeywell, India**

Personal & Hobbies:

- **Married. 2 Kids young enough to mess up the house and my work.**
- **Interested in Music and Sports.**
- **Like travelling**

Image Source: https://www.giac.org/certifications/web-application-penetration-tester-gwapt/
https://www.giac.org/certifications/penetration-tester-gpen/

Recent Vietnam Trip Glimpse (April 2025)

Disclaimer!!!

All the information presented in this slide is either publicly accessible/available or generated by me. The content I discuss reflects my personal opinions, and Honeywell holds no responsibility for any information utilized or shared during this session.

Agenda ~ 40 minutes

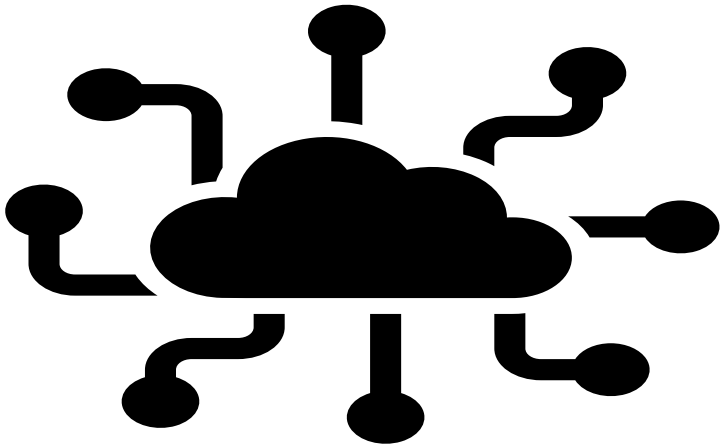
1. Safety & Security in avionics space – 5 min
2. Need for Connected Aircraft Use cases – 5 min
3. Connected Avionics Problem Domain- 10 min
4. Avionics Space Common threats & Security Controls/mitigations – 5 min
5. Regulatory considerations & Compliance in Aerospace Business – 5 min
6. Cybersecurity Rollover Challenges in Aerospace Business – 5 min
7. Quiz– 5 min

Safety & Security - Relevance in Aerospace

- Potential Safety Hazards identification and risk assessment
- Design & Implementation of mitigating measures
- Highest Design Assurance Level A, B, C developed Code
  (A - Catastrophic, B – Hazardous, C – Major)
- Extensive V & V of onboard avionics system

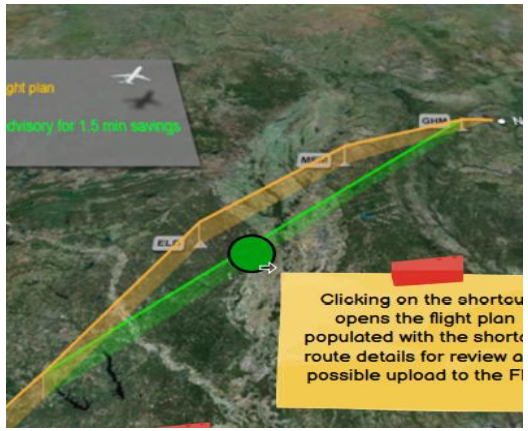
- Aircrafts are flying for decades
- Never designed to be ‘Secure’ but still doing fine
- Isolated and standalone, offered less features
- Manual labor intensive & less operational efficiency

‘Connected’



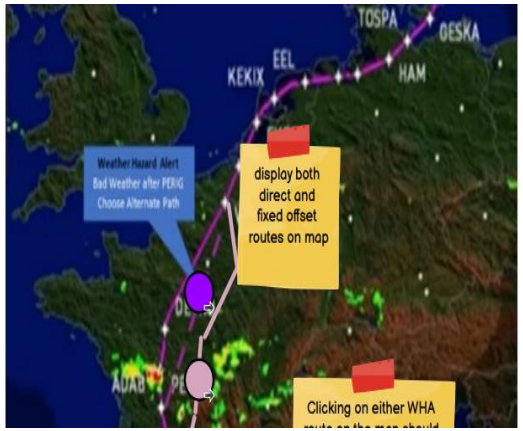
Aviation Cybersecurity Market size value in 2024 - ~10B Expected to grow to ~15B by 2030

Need for Connected Use cases in Aviation Sector



- **Short Cut Advisor**

- A feature that uses weather radar for computing shorter, faster, and/or less turbulent routes using known flight paths.
- The shortcuts will typically be based on previously flown paths using current conditions, so the probability of getting ATC approvals is high.
- The shortcut can then be quickly and seamlessly uploaded to FMS for ATC route clearance.

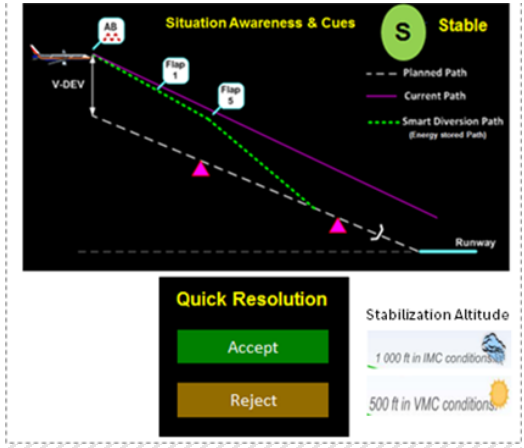


- **Weather Hazard Avoidance**

- A features that automatically identifies weather situations ahead and provides recommended course changes to avoid the weather via an integrated moving map.
- The feature will show high-fidelity routes unlike the generic guidance provided by ground services, making it possible for pilots to clearly evaluate the route and have more informed discussions with ground control.

- **Energy Management**

- A feature that provides guidance and situational awareness on the aircraft's ability to meet to achieve stabilized conditions at each gate along the descent path.
- It will perform an analysis of the current energy state for the remainder of the flight and recommend the actions needed to achieve stabilized conditions.

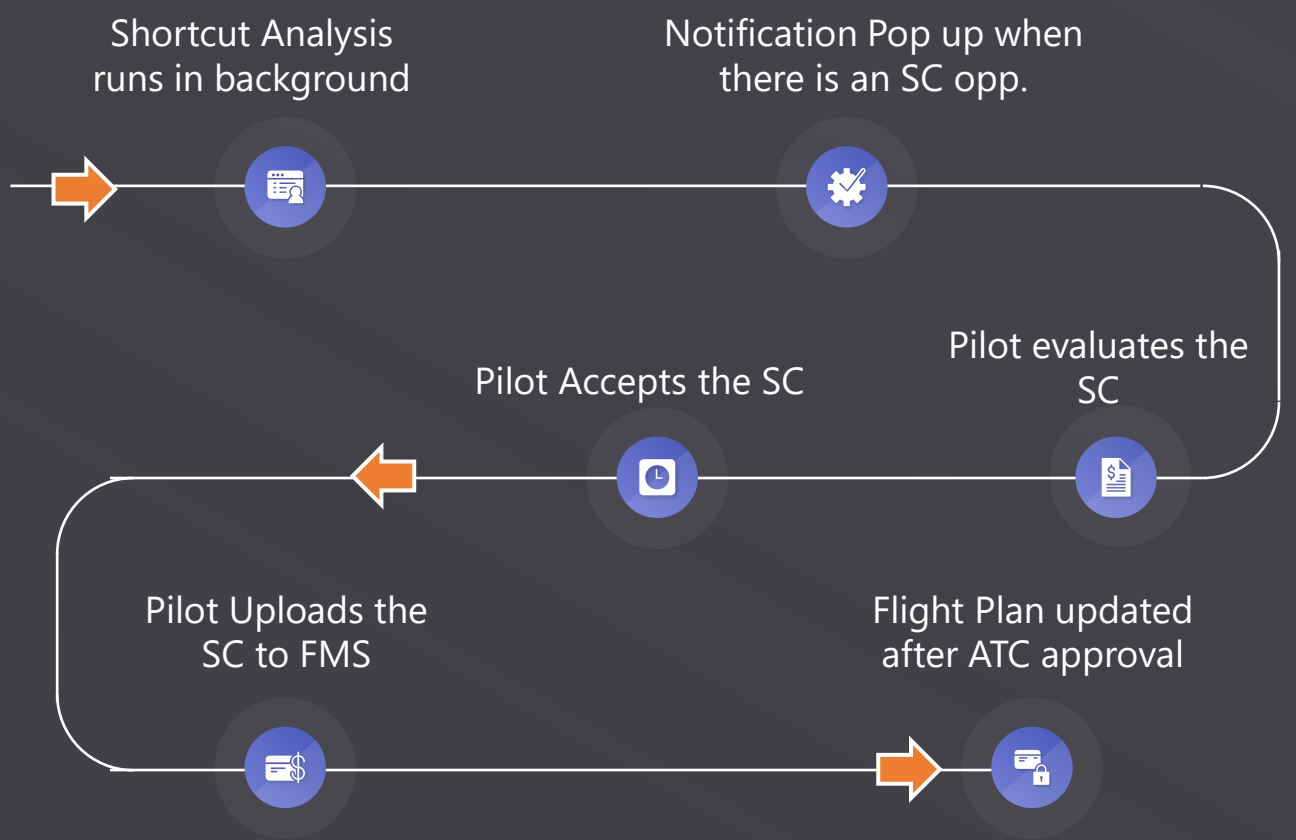


- **Last Moment Change**

- Provides pilots with a quick means of assessing stable landings for making landing or go-around decisions.

Shortcut Advisor

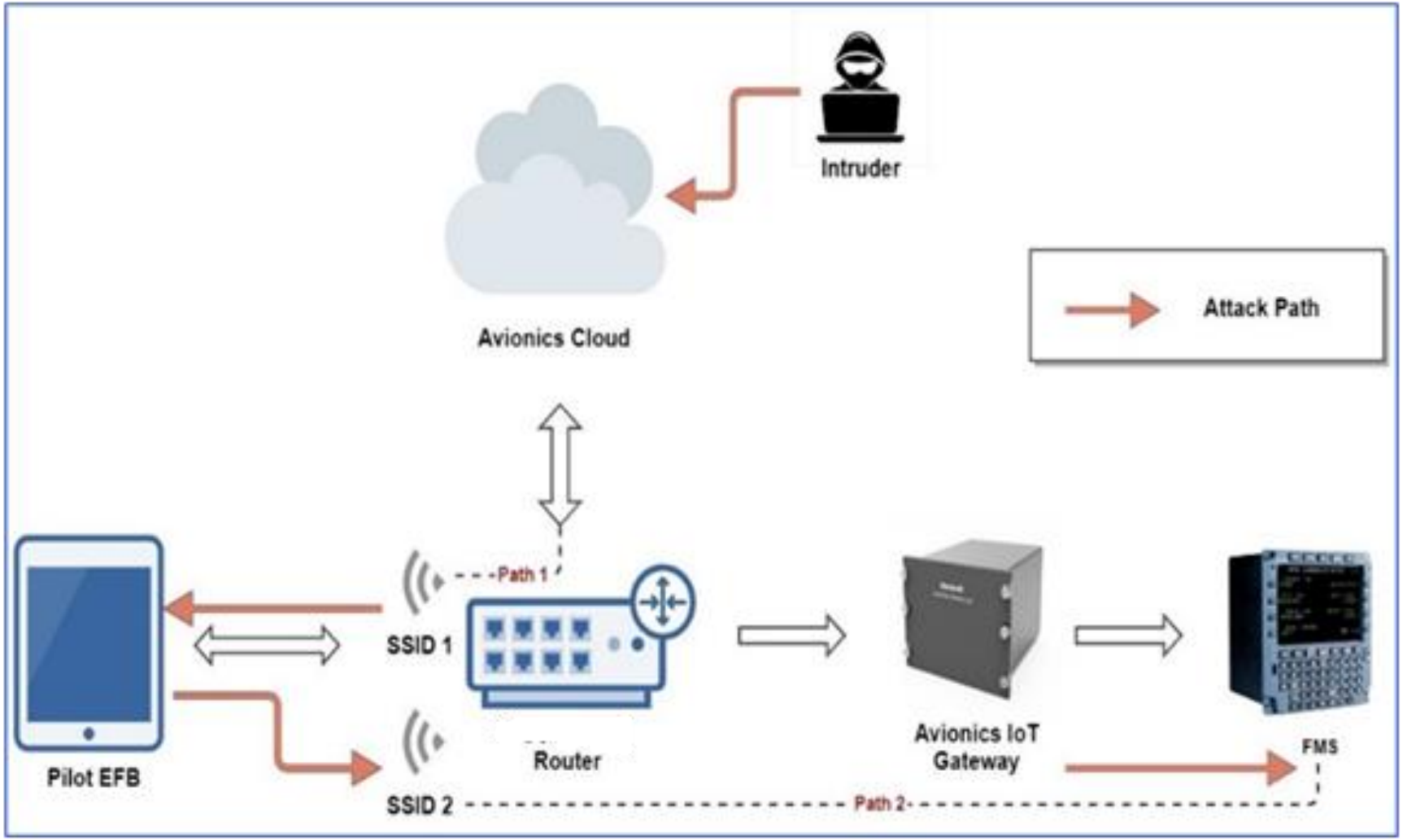
- A feature that uses weather radar for computing shorter, faster, and/or less turbulent routes using known flight paths.
- The shortcut can then be quickly and seamlessly uploaded to FMS for ATC route clearance.



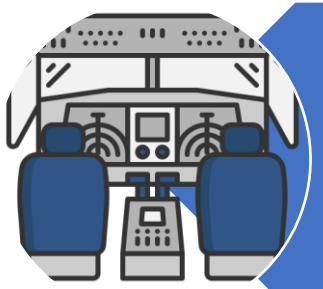
Benefits

Additional 2-3% fuel savings

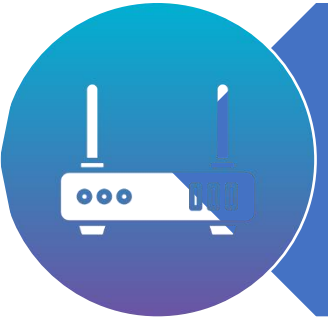
PROBLEM DOMAIN



Common Mitigations - Layered Approach

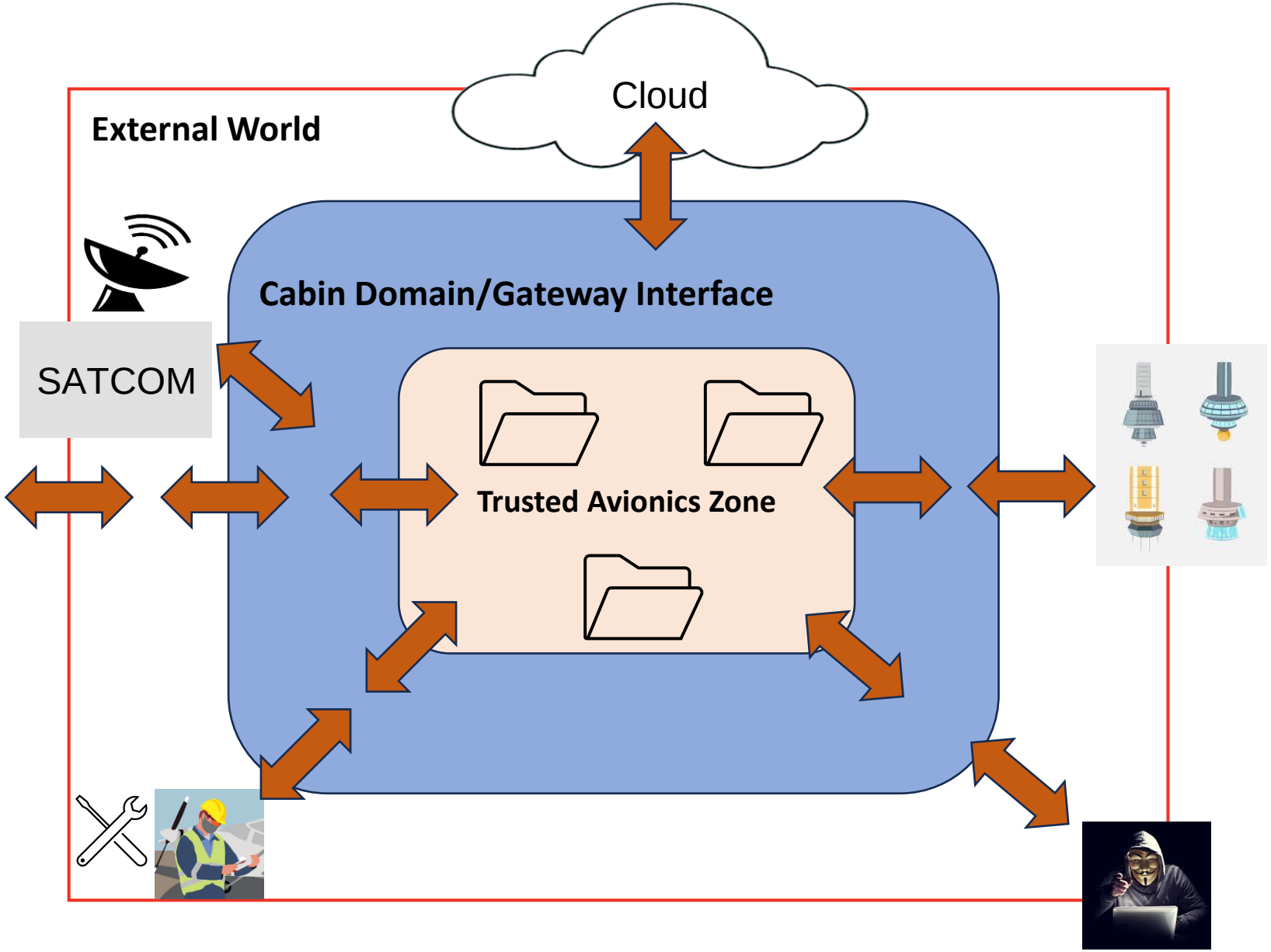


- Secure Boot
- Software Robustness
- Configuration Management



- Secure Boot
- Software Robustness
- Secure Communication
- Domain Separation

- Operational Security Measures
- Best Practices
- Awareness & Trainings



Regulatory Considerations In Aviation Sector

Process Specifications

- DO-326A/B/ED-202A Airworthiness Security Process Specification
- DO-356/ED-203 Airworthiness Security Methods and Considerations
- DO-355/ED-204 Information Security Guidance for Continuing Airworthiness

The above specifications are guidelines.

- The scope is only preventing the system from “IUEI”.
- These guidelines excludes physical attacks from their guidance.

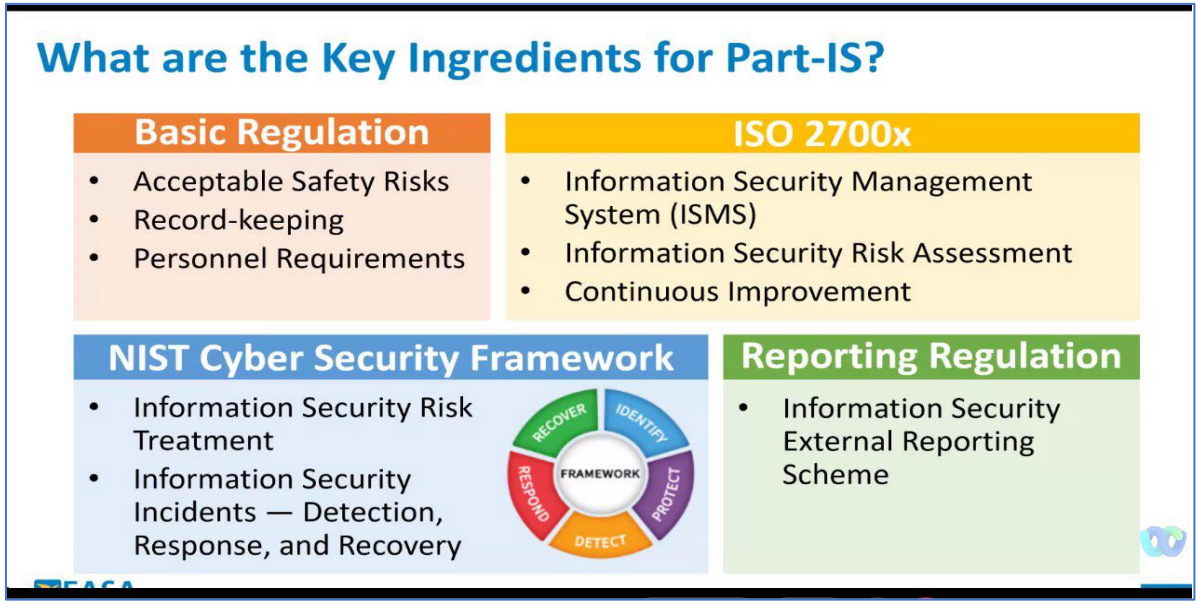
Biden’s Executive Order 14028:

- Strengthening the National Cybersecurity in Federal Agencies
- Removing Barriers between govt agencies & private sector in sharing sensitive information
- Improving Supply Chain Security

DO-326B is officially released during mid of 2024

Emerging Cyber Compliance in EU Region

- **Part IS:**
  - Objective: To protect the aviation systems from information security risks with potential impact on the aviation safety.
  - Scope: Airworthiness
  - Implementation: Published in 2022 and effective from mid of 2025



Cyber Resiliency Act:

- Strengthening Cybersecurity Standards
- Supply Chain Security
- Incident Reporting Requirements
- Increased Accountability and Liability
- Collaboration and Knowledge Sharing

Cybersecurity Challenges in Aerospace Sector

- Information Gathering on real cybersecurity incidents
- Nature of the Industry in terms of Sensitivity
- Pace at which change happens
- Large Legacy Code Baggage
- Dynamic Regulatory Landscape
- Geopolitical Conflicts

QUIZ – QUESTION - 1

- **Which organization or standard provides guidelines specific to aviation cybersecurity, addressing the risks posed by connected avionics and other digital systems?**

a) ISO/IEC 27001

b) DO-326A / DO-356A

c) PCI-DSS (Payment Card Industry Data Security Standard)

d) NIST (National Institute of Standards and Technology) Cybersecurity Framework

- **The answer is: b**

QUIZ – QUESTION - 2

- **An avionics system transmits real-time data via satellite communication networks and interacts with other aircraft systems. Which of the following threats are most critical to ensure secure communication in connected avionics systems?**

1) Spoofing attacks
2) Man-in-the-middle (MITM) attacks
3) Unauthorized physical access
4) Malware injection
5) GPS jamming

- **The answer is: 1, 2, and 5**

QUIZ – QUESTION - 3

- **To prevent cyber vulnerabilities in avionics, layered security architectures are employed. Which combination of layers would provide the highest protection?**

1) Secure boot processes in hardware systems
2) Application firewalls on avionics software
3) Secure network segmentation for onboard systems
4) Data logging and anomaly detection mechanism

a) 1, 2, and 3
b) 2, 3, and 4
c) 1, 3, and 4
d) All of the above

- **The answer is: d) all the above**

Questions?

Q & A

Thank You