Cybersecurity and Business Aviation

EASA Business Jet Workshop

January 2025

GARMIN®

Business Jet Landscape

Part/CS 23 L II-L IV, Part/CS 25

Characteristic	Smallest	Largest
Seats	Up to 7	Up to 19 pax, 3 crew
Range	~1,200 NM / ~2230 km	~8,000 NM / ~14,800 km
MTOW	6,000 lb / 2,720 kg	105,600 lb / 47,900 kg

- Support Part 91/Part-NCO, Part 135 or Part-CAT/ORO operations
- Maintenance: Factory service centers, 3rd party MRO/CAMO

Aviation Cybersecurity

Almost 20 years of progress

- 2007: First special conditions, IPs, CRIs
- 2007: Standards work begins via RTCA SC-216, Eurocae WG-72
- 2010: DO-326/ED-202 published
- 2014: DO-326A/ED-202A published
- 2014: DO-356 and ED-203 published (not harmonized)
- 2015: ASTM standards work begins for Part 23 aircraft
- 2016: FAA ARAC ASISP report published
  - Recommendations for specific rules
  - Task to harmonize DO-356 and ED-203 content
- 2018: DO-356A/ED-203A published (harmonized)
- 2020: EASA rules for aircraft, rotorcraft, engines published
  - Rules applicable from Jan. 1, 2021
- 2022: ASTM F3532 published
- 2024: FAA NPRM for large aircraft, engines

GARMIN.

The Broader Landscape

Rapid changes in areas outside aviation

- EU Radio Equipment Directive
  - Devices with direct or indirect internet connections
  - Applies beginning August 2025
- EU Cyber Resilience Act
  - Apps and services, plus devices
  - Software and hardware components
  - Vulnerability reporting
  - Applies beginning December 2027
- US Cyber Trust Mark
  - Devices with direct or indirect internet connections
  - Voluntary, materials still in development
- Many others (e.g. EU NIS2, “Critical Infrastructure”)

Proportionality

Align with the safety continuum

- Use “Right-sized” processes
  - ASTM F3532 vs DO-326/ED-202 family
- Certification and change impact analysis
- Environmental assumptions
- Operational assumptions
- Risk identification and treatment

- EASA update: Good progress on ASTM F3532 end of last year for Part/CS 23 L I to L III aircraft
  - Vulnerabilities activities **without** testing for up to L III aircraft
  - Increasing requirements for security measures from L I to L III
  - Position harmonized with FAA

Maintaining Systems

- Many aircraft and systems predate current cybersecurity rules and standards
- Regulatory guidance – “major” changes step up to new means of compliance
- Leverage change impact analysis for narrow fixes or improvements at appropriate level of effort
  - Make it simple to address vulnerabilities or field concerns
  - Avoid “perverse incentive” of new process requirements dissuading maintenance
  - New data flows get new scrutiny