2025 Civil Aviation Cyber Security Annual Report

Given to the AIA Civil Aviation Council 2025

Civil Aviation Cybersecurity Subcommittee

Stefan Schwindt – Chair (GE Aerospace)
Sean Sullivan – Chair (Boeing)
Stewart D'Leon – AIA Leader
Patrick Morrissey – Editor (Collins Aerospace)

Contents

1 INTRODUCTION

The Aerospace Industries Association (AIA) Cybersecurity Subcommittee is a dedicated community of experts representing aircraft manufacturers and their suppliers within the aerospace industry. Our members collaborate to foster discussion, identify shared interest, and advocate for regulatory and standards updates. This subcommittee aims to ensure the industry's continued safe and secure operation while encouraging innovation. To this end, the subcommittee has continued to work on the topics considered to be the highest priority based on discussions amongst industry stakeholders including pilots, operators, and manufacturers. This paper contains a summary of standards and regulatory updates which are important to industry, as well as a summarized position paper drafted by the subcommittee in 2025.

2 Regulatory Updates

2.1 Brazil (ANAC)

The National Civil Aviation Agency of Brazil (ANAC) has taken a coordinated, policy-driven approach to advancing cybersecurity across the aviation sector. Aligning with ICAO guidance and Brazil's national cybersecurity strategy, ANAC established its Cybersecurity Committee in 2023 to lead key initiatives such as developing the Sectoral Cyber Incident Management Plan, centralizing incident notifications, promoting aviation cybersecurity policies, and ensuring harmonization with federal and international standards. ANAC integrates cybersecurity into regulatory frameworks for both airline and airport operators through RBAC 107 and 108, requiring risk-based protection of critical ICT assets and ensuring that cyber measures are embedded in operator security programs.

To support the sector, ANAC publishes technical and guidance materials including manuals on cybersecurity awareness, assessments, and information sharing, drawing on ICAO's global cybersecurity guidance. The agency also maintains a dedicated incident reporting channel and is developing new regulations to formalize cyber incident management requirements. Recent efforts include a pilot program assessing cybersecurity maturity at selected airlines and airports using CIS Controls v8, along with ongoing oversight of compliance with existing cyber-related regulations. Looking forward, ANAC's roadmap emphasizes stronger information sharing, further international harmonization, development of new regulatory instruments, enhanced cybersecurity culture across the industry, improved training, data protection in emerging technologies like biometrics and AI, and greater resilience of critical aviation infrastructure.

2.2 U.S. (FAA)

In August 2024, the Federal Aviation Administration (FAA) released a Notice of Proposed Rulemaking (NPRM) which includes Aircraft Systems Information Security Protections (ASISP) for 14 CFR Part 25 category aircraft as well as 14 CFR Parts 33 (engines) and 35 (propellers). The comment period for the NPRM closed on October 21, 2024. These comments have been resolved. The final rule is progressing and is expected to be published in the second half of 2026. A draft Advisory Circular (AC) will also be published concurrently with the rule and provides the Accepted Means of Compliance (MoC), referring to the industry standards generated by RTCA SC-

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928 | 703.358.1000 | www.aia-aerospace.org

216 and EUROCAE WG-72. In the meantime, special conditions continue to be applied until rulemaking activity is complete. The FAA has also updated issue papers to reflect current ASISP trends.

Network information security for Parts 23, 27, and 29 may use either the RTCA standards or the F44 ASTM ASISP standard (F3532) as a Means of Compliance (MoC), after an update is published in 2025. For both Parts 27 and 29, ASISP is addressed through the traditional XX.1301 and XX.1309 rules. For Part 23, ASISP is addressed by having new applicants step up to amendment 64 rules 23.2500, 23.2505 and 23.2510, while the rule basis for aircraft certified prior to Amendment 64 will remain 23.1301 and 23.1309.

The 2024 FAA Reauthorization Bill, enacted in May 2024, includes two provisions which will impact the FAA in the coming years. The first is section 392, which amends the FAA's authorities under Title 49 of the U.S.C. by explicitly including cybersecurity as part of their responsibilities to ensure the safety of civil aircraft, engines, and propellors. In addition, this section provides FAA exclusive rulemaking authority within the federal government to issue regulations that address the cybersecurity of aircraft, engines, and propellers. The second provision is section 395, which directs FAA to establish a Civil Aviation Cybersecurity Aviation Rulemaking Committee (ARC) within one year of the enactment of the Reauthorization Act and includes a list of considerations that the ARC may include within its scope. In compliance with the regulation the ARC assumed their mandate with a first meeting in June of 2025.

2.3 U.K. (UKCAA)

In 2025 the UK Civil Aviation Authority (UKCAA) introduced several regulatory updates to address advancements and challenges in both manned and unmanned aviation.

For manned aviation, the Cyber Security and Resilience Bill, currently in its second reading in Parliament after being introduced on 12 November 2025, represents a significant step forward in safeguarding the aviation supply chain. While the Bill does not replace the Network and Information System Regulation from 2018, it introduces new requirements, such as granting the UKCAA the authority to designate critical suppliers and bring them under the scope of the regulation. This initiative aims to bolster the security and resilience of civil aviation operations (Link). Additionally, UKCAA has established an AI Strategy & Portfolio Hub to serve as its central function for managing artificial intelligence initiatives. This hub acts as a focal point for engagement with government, industry, and the public, while also shaping and leading UKCAA's regulatory activities on AI in aviation. Another major development includes the proposal to regulate ground handling services at UK-certified and licensed aerodromes which seeks to improve safety and foster collaboration among airlines, aerodromes, and Ground Handling Service Providers (GHSP)(Link). To this end, UKCAA published "CAP-3183" in October 2025 for public and industry consultation.

In the realm of unmanned aviation, UKCAA continues to play a leading role in international regulatory collaboration as the global secretariat for the Joint Authorities for Rulemaking on Unmanned Systems (JARUS). JARUS recently released version 2.5 of the Specific Operations Risk Assessment (SORA), which UKCAA has not only adopted but also adapted with additional cybersecurity enhancements. These adaptations are presented

in a Guidance Material/Acceptable Means of Compliance (GM/AMC) format and were published as "CAP-3098" in September 2025 for public and industry feedback (Link).

These initiatives underscore UKCAA's commitment to maintaining safety, security, and innovation in the aviation sector, while fostering collaboration with stakeholders across government, industry, and the public.

2.4 E.U.

EASA is expected to publish CS-23 Amendment 6 together with updated AMC & GM to CS-23 Issue 5 in the first half of 2026. The update clarifies acceptable means of compliance with CS 23.2500(b) regarding protection against intentional unauthorized electronic interaction (IUEI). For assessment level IV airplanes, applicants may consider AMC 20-42 (ED-20X standards), while for levels I–III, ASTM F3532-25 may be used. Certification level 1 airplanes operated in VFR (day or night) are not required to consider cybersecurity threats as sources of improper functioning.

Part-IS became fully applicable on 22 February 2026. The updated Easy Access Rules Easy Access Rules (Link), including cumulative amendments and GMs, have been published in December 2025. A Part-IS workshop is planned for 7–8 October 2026, while the dedicated Task Force of EU CAAs (including EASA) is developing or updating guidance for the harmonization of the oversight activities. In parallel, the Aviation Cybersecurity Subgroup has developed a "Mapping of EU cybersecurity rules applicable to the aviation sector," endorsed by the NIS Cooperation Group and shared with stakeholders to support regulatory harmonization.

3 Subcommittee Whitepapers

To provide guidance and direction to industry participants and leaders, each year the AIA Cybersecurity Subcommittee drafts papers with content sourced from a community of Subject Matter Experts (SMEs) which make up the subcommittee membership. This section provides a summary of the papers drafted this year.

3.1 Civil Aviation Operational Technology Recommendations Report (Link)

Within Civil Aviation, the Aerospace Industries Association (AIA) is seeing much increased use of OT in all facets of air and ground operations including air traffic management, as well as the fabrication, production, maintenance, and testing of aviation products and services. At the same time, OT systems are becoming more vulnerable to attacks due to increasing connectivity and exposure to internet facing networks, cloud-hosted environments, and data sharing with other IT/OT devices and communications systems. If not adequately protected, OT vulnerabilities can be exploited by threat actors and result in potentially critical impacts to human safety, the environment, brand/reputation, quality, and the resilience of civil aviation air and ground operations. In response to the growing importance of OT to Civil Aviation, the Aerospace Industries Association (AIA) Civil Aviation Cybersecurity Subcommittee has developed this report to provide strategic recommendations for enhancing the cybersecurity of OT systems within the civil aviation sector.

4 Standards Updates

4.1 RTCA SC-216 / EUROCAE WG-72 (Link)

In 2025, ER-039/RR-005 Report on Aviation Data Security and ER-040/RR-007 Information Security Management System (ISMS) for Aviation Organizations were published. The committee continues its pursuit of a more resilient aerospace system through the Terms of Reference (TOR) which can be found through the link in the heading.

4.2 Artificial Intelligence and Machine Learning (AI/ML)

AI/ML continues to be an important emergent topic in aerospace with multiple industry organizations hosting discussions to understand both risks and the associated mitigations. Together SAE G-34 and EUROCAE WG-114 initiated a new subgroup on the topic of cybersecurity through SG9. On August 5, RTCA held an AI/ML in ATM hybrid workshop in Washington DC. FAA held an AI/ML Roadmap and Technical Exchange Meeting. EASA held AI Days August 27-28. While there is a lot of interest in AI/ML in aviation, and safety topics are being discussed in these forums, cybersecurity needs more attention.

4.3 Internet Protocol Suite

The SC-223 TOR was updated and approved by the PMC. SC-223 and WG-108 will be publishing a technical report in 2026 which will outline the changes that need to be made to the IPS MASPS (DO-404) and Profiles (DO-379A) based on the outcomes of the IPS validation activities currently in-progress (i.e. the FAA IPS Very Large Demo in the US and some of the SESAR sub-projects in Europe).

Related to IPS is AEEC Hybrid Communication Network (HYCON). HYCON Specification 860: Hybrid Communication Network (HYCON) for Aeronautical Safety Services will include five parts: Concept of Operations (CONOPS), System Technical Requirements (Airborne), System Technical Requirements (Ground), and Protocol.

4.4 ICAO

Several ICAO panels are actively engaged in cyber-related initiatives to strengthen aviation security and digital trust. The ICAO Cybersecurity Panel (CYSECP) is leading efforts to implement the Aviation Cybersecurity Strategy and Action Plan and is currently developing the “Manual on Aviation Cyber Security,” which will offer guidance on incident response, vulnerability management, patching, and related topics, with publication expected in 2026. In parallel, the ICAO Trust Framework Panel (TFP) plans to publish Doc 10169, the Aviation Common Certificate Policy (ACCP), by the end of 2025 and is also preparing the “Manual on Trust Frameworks” to support implementation of the ACCP and other trust-framework-related documents under development. Within the ICAO Communications Panel, working groups DCIWG and WG-I are finalizing several IPS security standards (Doc 10090, Doc 10095, and Doc 10145) along with the third edition of the IPS Manual (Doc 9896), expected in early 2026. WG-I will subsequently update Doc 9896 to incorporate VoIP for

aeronautical communications as part of the fourth edition, and the group will begin developing HYCON standards, including a security assessment. Additionally, the ICAO Task Force on Cybersecurity Standards and Recommended Practices (TF-CYSARPS) continues work to enhance cybersecurity-related Standards and Recommended Practices across the aviation sector.

4.5 Other Cyber-Related Standards

4.5.1 Airlines for America

AIA monitors Airlines for America (A4A) and other operator related activities for communication and alignment between manufacturers and operators regarding aviation cybersecurity.

4.5.1.1 ATA Cybersecurity Working Group (Link)

Formerly known as the ATA Digital Security Working Group, the ATA Cybersecurity Working Group (CSWG) is preparing updates to ATA Spec 42 for release in 2026. Key areas of work include incorporating post-quantum computing considerations, deprecating the Time Stamp Authority and the Reference Digital Signature Policy, and introducing Secure Boot capabilities independent of a TPM. The group is also developing a Spec 42 training module and engaging in broader discussions on topics such as crypto-agility, appropriate use of time-stamping, and PIV-AV.

4.5.2 ASTM Systems and Equipment Subcommittee (Link)

F3532-25 was published August 29. FAA and EASA intend to accept it for Part 23 Level I-III. FAA also accepted -22 for Level IV. The next goal is to develop material for Level IV. They are targeting a mature draft mid-2026 with a new ASTM WK number assigned.

4.5.3 Airlines Electronic Engineering Committee

The Airlines Electronic Engineering Committee's (AEEC) group of committees and working groups develop engineering standards and technical solutions for aircraft systems to improve efficiency while reducing the lifecycle cost.

4.5.3.1 AEEC Users Forum

AEEC has set up an industry group known as the Cyber User's Forum in 2024 to provide a venue for operator concerns on cybersecurity. The inaugural meeting was held in Detroit, Michigan in April 2024. The forum was well attended by both operators and manufacturers. The event is planned to occur annually. The most recent ones occurred March 11-13, 2025, in Munich, Germany and March 10-12, 2026, in Charleston, South Carolina.

4.5.3.2 AEEC Software Distribution and Loading Subcommittee (Link)

The AEEC Software Distribution and Loading (SDL) Subcommittee is progressing several key deliverables across multiple ARINC standards. For ARINC 645-2, after re-evaluating the three existing software-signing methodologies aligned to Boeing, Airbus, and Carillon, the group agreed that only software parts (not the distribution crates) are installed on the aircraft, reaffirming that crates function solely as distribution

mechanisms. Work on ARINC 851 has expanded to include broader guidance for secure ground-system software distribution and new definitions for all categories of Aircraft Relevant Software, along with refined objectives and scope. The subcommittee is also developing updates to ARINC 615A to address requirements for software loading over Wi-Fi in response to a request from the ARINC Cabin Systems Working Group. Draft updates to ARINC 835 Supplement 2 now include a third signing method, considered method C. Methods A and C incorporate timestamps and OCSP validation. Discussions are ongoing about whether a single tool could be created to validate all three approaches. Adoption Draft 3 is currently available. Similarly, ARINC 827 Supplement 2 is being updated to include two signing methods: Method 1, which signs the crate, and Method 2, which does not sign the crate but relies on software-part signatures. The team continues to evaluate combinations of signing and creating methods. Adoption Draft 3 is also available for this standard.

4.5.3.3 AEEC Network Infrastructure Cybersecurity & Security Subcommittee (Link)

The AEEC NICS Subcommittee has been renamed NICS to underscore its growing focus on cybersecurity, and it is actively advancing several deliverables along with a new APIM. Project Paper 857, which addresses the security of non-safety SATCOM communications and considers integration with IPS and a hyperconnected ATM environment, has its first draft available. Similarly, ARINC Report 852, providing guidance for security event logging in an IP environment, has Draft 1 completed. The subcommittee continues working to define logging guidance for ACD and PIES, including log-message generation and analysis needs. Updates to ARINC Report 811, covering Commercial Aircraft Information Security. Part 1 provides concepts of operation while Part 2 focusses on risk assessment methodologies. The first draft for Part 1 and the second draft for Part 2 are available with completion targeted for April 2026 at the ARINC General Session. In early-phase discussions, a new APIM is being shaped, including proposed updates to ARINC 822 on on-ground aircraft wireless communication focusing on IPv6, authentication, and Wi-Fi/cellular protocols with midterm approval anticipated in October 2025. Additionally, updates to ARINC 664 Part 5 are underway, shifting from a domain-model approach to a security-zone model, with work aimed toward April 2026.

4.5.4 SAE

4.5.4.1 SAE S-18 Aircraft and Systems Development and Safety Assessment Committee (Link)

The S-18 committee is working jointly with EUROCAE WG-63 on the aerospace information report AIR8480 Safety-Security Interactions. The report seeks to address cybersecurity and safety interactions at the systems level consistent with what's described in the EUROCAE and RTCA cybersecurity subcommittee standards documents already. This addition to the industry standards will further help ensure cybersecurity is properly incorporated into the system development process to ensure proper interactions between the two processes and trade-offs between the two subject areas are fully considered.

4.6 Standards Coordination

4.6.1 ECSCG (Link)

The European Cybersecurity for Aviation Standards Coordination Group (ECSCG) is a joint coordination and advisory body established to align cybersecurity-related standardization efforts across the aviation sector. ECSCG is currently advancing the European Rolling Development Plan strategy, aligned with the Union Rolling Work Programme for European cybersecurity certification, which emphasizes the use of standards, secure-by-design principles, risk-based assurance levels (Basic, Substantial, and High), and identifying areas for future certification expansion. Looking ahead, ECSCG's coordination role will encompass activities across both regulatory and standardization domains, including work conducted by EU and EASA authorities, EUROCAE, ASTM, ARINC/SAE, the ARINC Security Forum, ICAO, ENISA, IATA, SESAR, and ETSI.

4.6.2 US ACCESS WG

The purpose of the ACI US Aviation Coordination of Cybersecurity & E-enabled Standards Strategy (US ACCESS) Working Group is to collaborate with stakeholders across the aviation cybersecurity ecosystem to shape a U.S. strategy for aviation cybersecurity standards. The group provides coordinated U.S. input to standards bodies and works to identify and resolve duplicates, conflicts, and gaps within the broader standards landscape. Currently, the US ACCESS Working Group is concentrating on US-specific considerations, including standards used by the U.S. military, while also exploring opportunities for harmonization between U.S. and European efforts as well as between civil and military aviation. The group invites guest speakers to enhance awareness of emerging aviation cybersecurity topics among its diverse membership. Currently, the group is on hiatus until the Civil Aviation Cybersecurity ARC is completed.

4.7 Aviation Information Sharing & Analysis Center (A-ISAC) (Link)

There is a new Aircraft Cyber Security Working Group with the goal to develop an Aviation centric framework modeled after MITRE ATT&CK & SPARTA. One help needed is diversity of participants to include more OEM manufacturer support, e.g. AIA members. There is also a new AppSec COI with a similar help needed, diversity of participants as well as co-lead for COI.

The annual Summit was held in Zurich, Switzerland October 13-17 in conjunction with the Q3 AvTech. The next one will be held in Vancouver, BC, Canada September 29-October 2, 2026.

5 Future Work and Considerations

5.1 Research Supported by AIA

When AIA established the Civil Aviation Cybersecurity Subcommittee, industry members identified cybersecurity risks to both aircraft and the aviation manufacturing environment as critical priorities. In response, the FAA created the Cyber-Security Data Science (CSDS) research program to address these needs and strengthen cyber-resilience across aircraft systems and manufacturing operations. Throughout 2025, AIA

continued supporting collaborative workgroups with the CSDS program to explore the application of AI and machine-learning concepts in aviation manufacturing environments. AIA members also partnered with airline operators in a parallel CSDS workgroup analyzing aviation data sets derived from aircraft logs. These efforts resulted in proof-of-concept demonstrations, technical findings, and recommendations that contributed to standards development activities such as ARINC 811, ARINC 852, DO-392, and ongoing RTCA and EUROCAE work.

AIA's industry-government collaborations align with the 2025 Presidential and DOT priorities aimed at enhancing the cybersecurity posture of the aviation sector. AIA recommends continued FAA support and government research funding to keep pace with evolving cybersecurity needs. Ongoing CSDS research remains valuable by bringing together government and industry expertise to improve the safety and resilience of aviation systems for the flying public.

Key findings from the manufacturing and operations workgroups emphasized that AI-ready data collection is essential for successful machine-learning analytics; ML techniques can effectively identify anomalies when supported by high-quality data and sufficient optimization; and sensor data must be relevant and, in some cases, refined for the intended analytical tasks. Corresponding recommendations included investing in AI-ready operational technology (OT) data collection, expanding OT analytics development, and sharing OT data to foster experimentation and advance analytics capabilities across academia and industry. Expanded collaborative work with airline operators also identified methods for reducing false positives in aircraft log analysis and provided insights into the time and resources required to train models to detect both field-level and structural anomalies. All findings and recommendations were published in restricted-access reports.

Appendix A: Members & Contributors

AIA Working Group Members:

Mayank Agarwal	Infosys	Patrick Morrissey	Collins Aerospace
Ruchik Amin	GE Aerospace	Siobvan Nyikos	Boeing
David Almeida	LS Technologies	Rose Poole	Shift5
Steve Benham	GE Aviation	Anup Raje	Honeywell
Majed Bouzouita	Boeing	Kanwal Reen	Collins Aerospace
Candice Burke	Boeing	Wes Ryan	Northrup Grumman
John Bush	Boeing	Aneesh Sankruth	Gulfstream
Don Christie	Honeywell	Dustin Scheller	Skygrid
Brian Connolly	Boeing	Stefan Schwindt	GE Aerospace
Michael Cook	ATI Metals	Sarah Stern	Boeing
Kathleen Finke	Astronautics	Sean Sullivan	Boeing
Marshall Gladding	Boeing	Nora Tgavalekos	RTX
Robert Hood	Astronautics	Jason Timm	AIA
Dave Jones	Astronautics	Jeff Troy	A-ISAC
Theodore Kalthoff	Archer	Michele Tumminelli	Gulfstream
Laurel Matthew	Boeing	Mike Wiegand	Shift5
Steven Marchegiano	ADI American Distributors	Mike Vanguardia	Boeing
Charles Minor	Pratt & Whitney	George Vergara	Raytheon
Alimuddin Mohammad	Boeing		

Cyber Working Group Guests/Observers:

Andrew Arnott	Airforce	Gernot Ladstaetter	Airbus
Jeffrey Burkey	FAA	Samantha Lopresti	FAA
Stephane Chopart	Airbus	Sam Masri	Honeywell
Diessner Daniel	Embry Riddle	Paul Nelson	Nelson Technical Associates
Harvie David	ERAU	Thomas Parmer	FAA
Gabe Elkin	MIT Lincoln Lab	Steve Ramdeen	FAA
Sidd Gejji	FAA ACI Tri Chair	Ted Rush	FAA
Vitaly Guzvhva	ERAU	Randy Talley	ACI Tri Chair
Denise Hampt	AirForce	Vincent Varouh	NASA
Jerry Hancock	Inmarsat	Isidore Venetos	FAA - Research
Clifford Jayson	Embry Riddle	Lauren Warner	Embry Riddle
Theodore Kalthoff	Bombardier	Philip Windust	FAA
Garfield Keith	ERAU	Hank Wynsma	United Airlines