Civil Aviation Cyber Security Annual Report

Given to the AIA Civil Aviation Council December 2024

Civil Aviation Cybersecurity Subcommittee

Stefan Schwindt – Chair (GE Aerospace)
Sean Sullivan – Chair (Boeing)
Chad Kirk – AIA Senior Director – Civil Aviation
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.

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

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 2024.

2 Regulatory Updates

2.1 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. After these comments have been resolved; the rule is expected to be published before Q1 2026. A draft Advisory Circular (AC) has also been published concurrently with the rule and provides the Accepted Means of Compliance (AMC), referring to the industry standards generated by RTCA SC-216 and EUROCAE WG-72. In the meantime, the FAA has 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[1] (ARC) within one year of the enactment (May 2025) of the Reauthorization Act and includes a list of considerations that the ARC may include within its scope.

2.2 E.U.

The European Union Aviation Safety Agency (EASA) has published a new Certification Memo (CM-21.A/21.B-001) which is used to define EASA's level of involvement in product certification in the field of cybersecurity. This update adds cybersecurity as a Compliance Demonstration Item (CDI) through the inclusion of "Cybersecurity" as an applicable discipline for in attachment 6. This guidance is used for the determination of the Level of Involvement (LoI) for EASA in certification programs and helps ensure cybersecurity impacts have been adequately considered and reviewed during the certification process.

EASA also continues work on Part-IS through updates and revisions to the current acceptable means of compliance (AMCs) & guidance material (GMs). Examples are the adaptation of ENISA ECSF (European Cybersecurity Skills Framework to Part-IS for the Aviation domain and compliance guidelines for ISO/IEC 27001 certified organizations.

The tentative timeline for the new AMC/GM material shows as follows:

[1] An ARC is an advisory body which allows the FAA to work with industry and the public to improve FAA's rules, and most importantly allow FAA to obtain information and insight from those parties most affected by FAA's existing and proposed regulations.

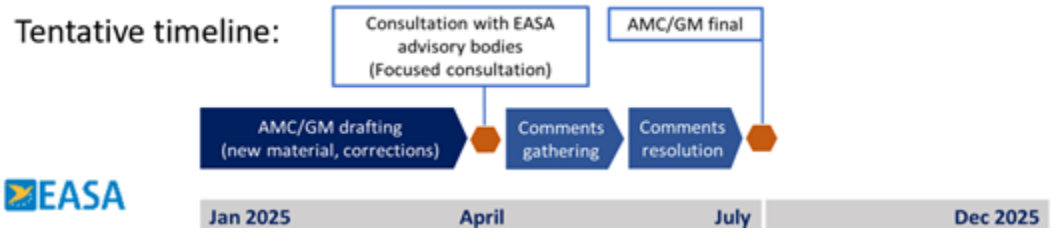

Figure 1: Part-IS AMC/GM Timeline

Additionally, the European Union (EU) has adopted or is in the process of adopting further non-sector specific regulation that may impact its members. The Network and Information Security Directive has been updated – commonly known as NIS2 – and now includes manufacturing of aviation parts and products as an "important entity" in addition to previous inclusion of airlines, airports, and air traffic control as "critical entities". The NIS2 directive was intended have been transposed into national law by all EU member states no later than October 2024 but, to date, it has not been completed by all countries.

The Cyber Resilience Act has introduced requirements for securing any products with digital elements. However, it's important to note the rule includes a carve out for products certified under EASA. The EU is also leading the way for Artificial Intelligence (AI) regulation. The Artificial Intelligence Act has been introduced to regulate AI and includes aspects of cybersecurity. The EU has requested EASA to establish sector specific implementation for AI and work is in progress to establish an aviation framework within Rulemaking Task 0742 in collaboration with AIA.

3 Subcommittee Whitepapers

In an effort 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 Software Bill of Materials (SBoM) (Link)

The purpose of this report is to provide recommendations to all aviation stakeholders – including government and regulatory agencies, aircraft operators, and aircraft manufacturers and their suppliers – on the implementation and utilization of SBoMs and related vulnerability identification and management within the civil aviation sector. The report addresses the need for updates to industry standards as well as developing new capabilities to maintain and share SBoM related information rapidly across the industry to facilitate both vulnerability and incident response.

4 Standards Updates

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

The RTCA and EUROCAE security committees (SC-216/WG-72) continue to work together on the development of standards for the industry to ensure common goals and outcomes. In June, the Terms of Reference (ToR) for SC-216 and the task sheet for WG-72 were updated to define the scope of work for the next two years. Below is a summary of the work currently underway by these committees on various standards:

- The B revision of DO-326/ED-202 (Airworthiness Security Process Specification) was approved by the respective committees and published in September. The new version fully harmonizes the two standards and updates the topics of security verification and Change Impact Analysis as it relates specifically to Information Security.
- A new report on Information Security Management System Guidance for aviation organizations are being drafted to provide guidance on the implementation of a management system for information security within organizations to supplement the safety management system and potentially serve as a means of compliance for Part-IS. A standard is planned to follow as industry understanding and approaches mature and harmonize the topic.
- Updates to DO-392A/ED-206A (Guidance on Information Security Event Management) are planned to address performance requirements for event reporting.
- A new report on Aviation Data Security is being developed to address minimum security standards for the generation, storage, and delivery of data which could impact the safety of the aircraft. A related standard is expected to follow as industry understanding and approaches mature and harmonize on the topic.
- For DO-356A/ED-203A:
    - A supplemental report will be developed to provide agreed upon answers for commonly asked questions and issues faced when using the standard to help ensure consistent interpretations.
    - The committee will also draft DO-356A/ED-203A Change 1 as a tightly scoped update to the existing DO-356A to reflect new supporting information for DO-356A.
- DO-355B/ED-204B (Information Security Guidance for Continuing Airworthiness) is planned to be updated to provide clarification of responsibilities and additional objectives for continued airworthiness security.

4.2 WG-112 eVTOL Cybersecurity

EASA has published the framework SC-VTOL (Special Conditions Vertical Takeoff and Landing) for certifying the new eVTOL (electric vertical take-off and landing) aircraft in development. From a security perspective, this framework aligns with CS-25 for large airplanes. EUROCAE WG-112 has been established by European industry to develop standards specific to eVTOL and is currently developing ED-305 as the cybersecurity guidance. The intent of ED-305 is to adapt ED-202 and ED-203 for use in the eVTOL space by adding guidance for eVTOL unique aspects and tailor compliance requirements for the risk profile of eVTOL aircraft compared to large airplanes. WG-72 member organizations have raised some concerns around the tailoring of objectives for security assurance levels by WG-112 for the ED-305 standard. These discussions are in progress and WG112 has taken these comments and various proposals under consideration

This work is not harmonized with the U.S. and therefore concurrent work is not being done with SAE or RTCA. The FAA intends for the ASTM F3532 standard to include eVTOL specific guidance in future revisions as the FAA is considering eVTOL as a specific class of Part 23 aircraft.

4.3 Artificial Intelligence and Machine Learning (AI/ML)

SAE G-34 and EUROCAE WG-114 are working jointly to address Artificial Intelligence and Machine Learning (AI/ML) in aviation. They are developing Aerospace Recommended Practice (ARP) 6983 (Recommended Practice for Development and Certification/Approval of Aeronautical Safety-Related Products Implementing

AI) which is currently in draft. Subgroup 9 (SG9) of the committee has been setup to investigate the security aspects of AI/ML and consider guidance. Of consideration are threats such as data poisoning, model stealing/extraction, and confusing the neural networks used by AI/ML, etc.

4.4 Internet Protocol Suite

Internet Protocol Suite (IPS) refers to the set of protocols used for data communication in aviation systems, essentially standard internet protocols adapted for aeronautical applications, often focusing on safety-critical communication within the National Airspace System (NAS). IPS industry standards are developed and maintained by AEEC, RTCA, EUROCAE, and ICAO.

AEEC ARINC 858 P1, P2, and P3 which make up the IPS Air and Ground Technical Requirements (including security) were approved at the AEEC General Session May 23 for publication. The three parts of the standard are titled as follows:

- Part 1: Technical Requirements
- Part 2: IPS Gateway Air-Ground Interoperability
- Part 3: Common IPS Radio Interface Protocol

The RTCA DO-379A/ED-262A Technical Standard of Aviation Profiles for Internet Protocol Suite was approved for publication by RTCA PMC and EUROCAE TAC and published. The responsible committees, RTCA SC-223 and EUROCAE WG-108, are entering active monitoring mode until the flight trial validation concludes for FAA and EASA. Once testing is complete through the Very Large Demo, SESAR, and IRIS activities, the committee will begin working on revisions of DO-379A and DO-404 (MASPS) which will be updated to reflect the results of the validation.

The International Civil Aviation Organization (ICAO) has been working on complimentary standards related to IPS which are summarized amongst other initiatives in the following section.

4.5 ICAO

There are several ICAO groups working aviation cybersecurity or cyber-related tasks. The ICAO Communication Panel (DCIWG + WG I IPS Security Subgroup) met in June and delivered a suite of documents:

- Doc 9896 Ed 3. Manual on Aeronautical Telecommunication Network (ATN) using IPS
- Doc 10090 Manual of Security Services for Aeronautical Communication
- Doc 10095 Manual of PKI Policy for Aeronautical Communication
- Doc 10145 Manual of Security Risk Assessment for Aeronautical Communication

The group is now starting an inter-panel coordination activity which will elicit comments from other panels and working groups which will need to be resolved prior to publication.

The ICAO Cybersecurity Panel (CYSECP) is working on implementing the Aviation Cybersecurity Strategy and Action Plan and drafting the first edition of the Global Cyber Risk Considerations (GCRC) Document.

ICAO Trust Framework Panel (TFP) is working the following documents:

- Doc 10204 – Manual on Information Security (MIS)
- Doc 10169 – Aviation Common Certificate Profile (PKI)

ICAO Integrated Comm Nav Surveillance and Spectrum Task Force (ICNSS-TF) is working its Proposal for Threat Modeling of all Future SARPS using STRIDE.

4.6 Other Cyber-Related Standards

4.6.1 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.

4.6.1.1 A4A Aircraft Information Security Program Working Group

The A4A Aircraft Information Security Program Working Group (AISPWG) is working on a D301 position paper which will contain recommendations and proposals for alignment on aircraft cyber processes across operators to help ensure consistency and uniformity across operators, industry, and regulators. As most US operators have aircraft network operational security program (D301s) certification renewals over next few months the motivation to complete and release the position paper is high. An Initial draft was expected to be completed by November 2024 with a likely release date in early 2025. At the AISPWG face to face meeting last November, the working group planned to provide feedback on AC-119-1A, NPRM & AC 20-xxx (the draft AC intended to accompany the FAA x.1319 regulations), threat scenarios and impact per ARINC 811 effort, ground system vulnerability management, design approval holder (DAH) plans for updating instructions for continued airworthiness (ICA) guidance, and the planned FAA Cybersecurity ARC.

4.6.1.2 ATA Digital Security Working Group (Link)

The purpose of ATA Spec 42 is to provide guidance for deployment of digital identity management solutions based on regulatory guidance. The Digital Security Working Group (DSWG) provides a forum to address the application of digital data security technologies and standards to ATA e-Business specifications. DSWG is working on the following guidance as part of the ATA Spec 42 update for 2025:

- Section 5.8 Credential Assurance Strength Recommendations will be updated to include digital signatures for all aircraft relevant software (as defined in ARINC 851). Assurance strength and key management guidance for keys used in secure boot will also be added.
- Spec 42 compliance assessment guidance - guidance will be added to help organizations that wish establish compliance with the ATA Spec 42.
- Post-Quantum Cryptography (PQC)/ Quantum-Safe Cryptography (QSC) guidance - a new appendix for PQC/ was added to the spec in revision 2024.1. This appendix will be updated in 2025 to add guidance on the use of Cryptographic Bill of Materials (CBOM) as an initial step to assess cryptographic use in products.

4.6.2 ASTM Systems and Equipment Subcommittee (Link)

The ASTM F44.50 subcommittee is working on updates to the F3532 standard (Standard Practice for the Protection of Aircraft Systems from Unauthorized Intentional Electronic Interaction) based on regulator feedback with a goal to have changes incorporated in 2025. As a first priority, Part 23 Level I-III aircraft work includes updating the assessment scorecard to include architecture and higher thresholds, adding language for vulnerability assessments, and clarifying system versus aircraft evaluation needs. For Part 23 Level IV aircraft, material is in development to address refutation testing and normal vs. enhanced assurance.

4.6.3 IAQG (Link)

International Aerospace Quality Group (IAQG) released AS9125 “Requirements for Aviation, Space, and Defense Organizations, Non-Deliverable Software”. It supersedes ARP9005, The Aerospace Guidance for Non-Deliverable Software, published in June 2005. Common training and checklists are planned. AI9115

"Requirements for Aviation, Space, and Defense Organizations, Deliverable Software" update is now in progress. Proposed improvements include Software Bill of Materials (SBoM). However, the schedule will significantly slip due to ISO delays coupled with a 9100 "Independent Review" driven by FAA/DCMA/NASA. A draft is not expected for review until October 2025 and a final release not expected until sometime in 2026.

4.6.4 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.

4.6.4.1 AEEC Users Forum

AEEC has setup an industry group known as the 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 with the next one planned for March 11-13, 2025, in Munich, Germany.

4.6.4.2 AEEC Software Distribution and Loading Subcommittee (Link)

The AEEC SDL committee develops and maintains standards for guidance around software loading and distribution. They are:

- ARINC 615A – Software Data Loading Using Ethernet Interface, which provides general and specific design guidance for the development of software data loading equipment for all types of aircraft.
- ARINC 645 - Common Terminology and Functions for Software Distribution and Loading provides airlines, airframe manufacturers, aircraft equipment suppliers, and others with information that is specific to data, software, and ground tools used in aviation configuration and data management.
- ARINC 665 - Loadable Software Standards, defines the aircraft industry's standards for Loadable Software Parts (LSPs) and Media Set Parts (MSPs). It describes the common principles and rules to be applied to any part of a data load system to ensure compatibility and inter-operability of software parts.
- ARINC 827 – Electronic Distribution of Software (EDS) by Crate describes the format for electronic distribution of aircraft software parts and other contents between aerospace business partners using a digital container referred to as an EDS crate.
- ARINC 835 – Guidance for Security of Loadable Software Parts using digital signatures provides background and detailed technical information on preferred methods to secure loadable software parts using digital signatures.
- ARINC 850 - System Level Guidance for Data Loading LRU Target Systems defines principles, concepts, and guidance for the design of data loading targets and complex data loading target systems.

The committee currently has three ARINC Project Initiation/Modification (APIM) in-process:

- APIM-23-009 Supplement 2 to ARINC 827 and 835: Updates to define a 3rd digital signature method (signed EDS Crate) in ARINC 835. Removal of digital signature details from ARINC 827, which will now be addressed in ARINC 835. ARINC 827 will define two methods of EDS (digitally signed and unsigned crate).
- APIM-23-003 Supplement 2 to ARINC 645: Supplement 2 will add additional guidance for users of ARINC 645-2 for PDL and ADL compliance and logging.

- APIM-22-004A ARINC Project Paper 851: Define standardized software distribution and receiving processes to help reduce the operational cost of acquiring software and securely distributing within an organization.

4.6.4.3 AEEC Network Infrastructure & Security Subcommittee (Link)

The AEEC Network Infrastructure and Security (NIS) subcommittee develops ARINC standards for secure broadband equipment interfaces, digital signature application, and a roadmap for introducing IPv6 into aviation. AEEC NIS is actively working revisions to three standards:

- ARINC 811 – Cyber Concepts and Risk Assessment have been proposed to be divided into two parts to preserve the original intent/content of the often cited document as well as address the operator concern for guidance on operator focused security risk assessments. The two proposed parts are:
  - Part 1 – Concept of Operations, this portion of the document will retain the original concept of operations with changes to reflect updates to the overall ConOps.
  - Part 2 – Risk Assessment Methodology: As ARINC 811 is targeted at the operator and not the OEM, the group is considering using NIST-800-30 as a baseline as opposed to the ASISP process, which aligns more with aircraft and system designers.
- ARINC 857 – Securing Non-safety Communication via Satcom is being developed in response to APIM 23-004. The standard is expected to consider systems which process non-safety but sensitive information, such as: PII and GDPR relevant data, PCI data, organizationally sensitive data, or maintenance information.
- ARINC 852 – Guidance for Security Event Logging is being revised to: align the content with updates to the DO-355A/ED-203A and DO-392/ED-206 standard, as well as expand the documents overall scope to consider security log guidance for the ACD domain, ground support equipment, and ground support information systems.

4.6.5 RTCA SC-236 Wireless Avionics Intra-Communication Committee (Link)

The SC-236/WG-96 Wireless Avionics Intra-Communication (WAIC) committees develop Minimum Operational Performance Standards (MOPS) for wireless equipment, allowing WAIC systems to share the radio spectrum with other aviation systems. WAIC MOPS are paused for release after receiving written replies from telecom organizations regarding the disposition of non-concurs on the spectrum protection elements. RTCA is working through dissent process from public, non-member commenters. In the meantime, SC-236/WG-96 is on active monitoring until further notice.

4.6.6 SAE

4.6.6.1 SAE G-32 Cyber Physical Systems Security Committee (Link)

The SAE G-32 Cyber Physical Systems Security Committee develops technical reports (Standards, Recommended Practices and Information Reports) covering a systems engineering approach to cyber physical systems security that includes analysis of the system operating environment defined by the operational, functional, and architectural systems engineering elements. The committee is currently working on JA6678 - Guidelines for Establishing and Maintaining Cyber-Physical-Systems' Cyber-Resiliency. There is no projected publication date currently.

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

The SAE S-18 Committee develops guidelines for processes, methods, and tools, to be applied at the systems and aircraft level describing interactions between various development processes between systems to bring

together the development of hardware, software, and systems components to support aircraft level certification. These guidelines include documents such as ARP4754, ARP5150, AIR6276. AIR6219, and ARP4761. The ARP documents are the main standards and are considered for update every five years. The AIRs (Aerospace Information Report) documents are lower level interim guidance or proposed updates to the community for consideration in the next update cycle of the main ARP. The S-18 Safety-Security Interactions Working Group has engaged with SC-216 and WG-72 to clarify the interactions between processes recommended by ARP4754B and ARP4761A with the security risk assessment and development process defined in the DO-326/ED-202 standard. The proposed material will be release as part of AIR8480 and should help clarify and standardize interactions between safety and security processes at the systems and aircraft level. AIR8480 is estimated for release in late 2025 or early 2026.

4.7 Standards Coordination

4.7.1 ECSCG (Link)

The European Cyber security for aviation Standards Coordination Group is a joint coordination and advisory group established to coordinate the cyber security for aviation related standardization activities. ECSCG is working on the European Rolling Development Plan strategy: Union Rolling Work Programme for European cybersecurity certification | Shaping Europe's digital future (europa.eu):

1. Use of standards
2. Secure by design
3. Risk-based assurance (Basic, Substantial, High)
4. Areas of future potential certification extension

Future coordination will cover activities done in the regulatory and standardization domains at EU/EASA, EUROCAE, ASTM, ARINC/SAE, ARINC security forum, ICAO, EU/ENISA, IATA, SESAR, ETSI.

4.7.2 US ACCESS WG

The purpose of the ACI US Aviation Coordination of Cybersecurity & E-enabled Standards Strategy (US ACCESS) Working Group is to engage and collaborate with cyber aviation ecosystem stakeholders on activities to establish a US strategy for aviation cybersecurity standards, provide a U.S. response to the Standards Coordination Groups, and identify and address duplicates, conflicts, and gaps in the aviation cybersecurity standards. The U.S. ACCESS WG has been focusing on the US only delta to include standards used by the US military, identifying opportunities for harmonization between U.S. and EU as well as civil and military aviation, and bringing in guest speakers to bring awareness of aviation cyber topics to its diverse audience.

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

This year marked the 10th anniversary of the A-ISAC which included 150 companies headquartered out of 26 countries; many more are in the process of membership application review. The 35th AvTech occurred in Germany hosting 140+ technical experts from around the world (designed to share risk mitigation solutions and all around best practices). The Annual Summit took place in New Orleans in September hosting a series of top speakers from private and public sectors; there will also be cyber challenge for college students. A-ISAC is now an operational "Follow-the-Sun model" delivering and hosting threat intel calls and WG sessions to all regions (APAC, Europe, Middle East and Americas). Multiple government stakeholders and entities are soliciting A-ISAC advice on cyber risk management that includes US, British, Israeli and Japanese governments. They are now offering free training tailored to the A-ISAC membership that includes MS Azure Security training, AWS training, MITRE ATT&CK and MISP training.

5 Future Work and Considerations

5.1 Cyber Aviation Rulemaking Committee (ARC)

The FAA Reauthorization Act of 2024 defined the establishment of a Cybersecurity Aviation Rulemaking Committee (ARC) in section 395 with direction to start in 2025. The structure of an ARC allows the FAA to work closely with industry to improve their rulemaking development and provide the FAA with the opportunity to obtain information and insight from those parties most affected by existing and proposed regulations. The scope of topics define by the Reauthorization Act was outlined in subsection 395(g) and was notably broad thus allowing for a wide scope of discussions. The final agenda still needs to be set by the FAA and is expected in Q1 of 2025. To further the AIA Cybersecurity Subcommittee's objectives of working towards regulatory harmonization and simplification this section provides a list of recommended topics to be included in the agenda.

Within the U.S., several cybersecurity regulations are being established through legislative acts and executive orders with oversight through different agencies. Through the ARC, the committee could explore how oversight of aviation organizations can be concentrated with the FAA as the prime agency. The FAA has the most detailed knowledge of the design, production, and manufacturing processes used by the industry (including AIA members) and how cybersecurity practices and rules would best interact with other regulatory constraints imposed by the FAA. By concentrating oversight of cybersecurity within the FAA, the potential burden of having different – and potentially conflicting – audits and directions from multiple agencies could be reduced.

Aviation is a global business, and it is also critical to consider activities in other regions. The European Union has issued Part IS with the UK to soon follow suit. Under the umbrella of ICAO, there is work underway on establishing an international cybersecurity framework for aviation. The ARC should use these datapoints in the discussions for recommending a US legal framework that allows AIA members to operate efficiently and effectively.

In the spirit of regulatory harmonization and simplification, AIA recommends the following topics to be included in scope of the Cybersecurity ARC:

- **Information Security Management System for aviation organizations**: The EU and UK Part IS rules require aviation organizations to establish an Information Security Management System, similar to the Safety Management System now required globally. ARC discussions can focus on whether the U.S. should introduce a similar mandate and to what degree as well as how international projects can be most efficiently managed.
- **Cybersecurity Aviation Safety Gap Review**: While the new rules to support cybersecurity for parts 25, 35, & 38 are progressing to ink, there are still gaps which should be considered and where additional rulemaking and standards might be useful to the industry. These include considerations for ground, ground supporting systems, data services, Air Traffic Management (ATM)/Air Navigation Services (ANS), Global Navigation Satellite System (GNSS), and AI/ML (mentioned below separately). While many of these systems are government provided services these systems may be dependent on private services provided by third parties which should be regulated accordingly.
- **Civil / military integration**: The U.S. military makes extensive use of aircraft initially certified with a civil Type Certificate (TC) and modified with military Supplementary Type Certificates (STC). The U.S. Department of Defense (DOD) uses a different framework (DODI 8510.01 vs DO326B and DO356A). A workgroup could be established on how the civil process can be accepted for modified aircraft as well as how it could be augmented to be used for military only aircraft.

- **Regulatory harmonization with other US agencies**: Several U.S. agencies have introduced cybersecurity requirements for organizations including the Security and Exchange Commission (SEC). These other rules are for general industry and have expectations to follow cybersecurity practices which violate safety principles and requirements in aviation. Therefore, it is necessary to establish security practices suitable for aviation organizations that can ideally be overseen by the FAA or used by other agencies as part of their specific oversight.
- **Protection of Design and Certification Data**: Regulations from the TSA call for security related design and certification documents to be marked as Sensitive Security Information to protect them from Freedom of Information Access (FOIA) requests. This is a US centric regulation which doesn't apply well to supporting documentation for commercial systems which have other protections under the control of private companies. Additionally, these documents, per other regulations, must be provided and delivered to operators both foreign and domestic. Conversely, some material released to the FAA should be reviewed for what it might reveal in a security context (such as STCs). A review of the certification process and supporting documentation should be done to consider how it should be classified to provide consistency across the international community which makes up the aerospace industry.
- **Software Signing**: Methods for assuring the integrity and authenticity of software running on modern systems is a mature and well defined area of process and technology. While OEMs are promoting this practice amongst their supply chain through contracts the time has come where the practice should be required across the industry. It will still be necessary for suppliers to incorporate solutions which make sense for their systems and business processes and discussions are needed to explore how broad the regulation should reach (Data items? Configuration files? Databases?). These days there are many components which are digitally delivered, and their origin should be guaranteed before installation.
- **Intelligence sharing between U.S. agencies**: Multiple law enforcement and security agencies collect, analyze and respond to incidents using data provided through the incident reporting process. Each agency has their specializations and particular strengths. It would be advisable to use these strengths to ensure an effective and efficient national response can be established to allow intelligence agencies to collect data and the FAA to provide inputs on criticality to the airspace.
- **Aviation cybersecurity vulnerability and incident reporting and response**: To date, no agreed method has been established to evaluate the risk impact of a vulnerability nor proposals of a consistent limit to response and how this might be considered differently for actual incidents. This topic has been difficult to resolve within industry committees and a fresh look at the topic might generate some new thinking. The Cybersecurity ARC could explore a common basis for the evaluation and reporting of vulnerabilities and incidents. In the safety discipline, the maximum allowable response time to defects and occurrences is calculated in a trapezoid considering: the severity of the defect, the probability or time to failure, the affected fleet size, and any temporary mitigations put in place that modifies these factors. A similar process should be established for security to establish how these safety vectors are impacted by vulnerabilities and incidents to ensure gaps are not left which could lead to undue harm. The ask is less about creating a singular method for evaluation but documenting what can feasibly be commonly applied across industry to help ensure common risk determination and safe resolution to issues.
- **Risk assessment methods**: The DO-356A standard used as an Acceptable Means of Compliance has multiple risk assessment methods as informational appendices rather than a single accepted method or multiple equivalent methods. Likewise, DO-355A does not provide a single or equivalent set of methods for the Airline Network Security Plans required for operators. The ARC could explore

equivalency and consolidation of risk assessment methods if the methodology is commensurate to the certification class of the system.

- **Federal Research and Development for aviation cybersecurity**: Cybersecurity is a continuously evolving field. While there is extensive research in the general field, there is little public research for the technologies used in aviation and the specific constraints found in this sector such as long lifecycles, real time operating systems and aversion to updates to maintain safety. Due to the criticality of aviation sector for public safety and both national and international economy, it would be advisable to consider where research and development can be directed for communal benefit.
- **Cybersecurity and Artificial Intelligence / Machine Learning**: Artificial Intelligence is new technology with promise of revolutionizing many sectors. Artificial Intelligence offers new capabilities to accelerate the design process, allow new operating modes for aircraft and enhance protections onboard aircraft. At the same time, it represents new potential vulnerabilities through the development process for design and operations as well new tools for the development of attacks external actors. While some regulators do not want to stifle innovation by regulating AI/ML, aviation is a safety critical sector with a risk averse posture expected by manufacturers and the public. As AI/ML can introduce threats that are not considered by the existing security processes, it is important to ensure that all approvals of AI/ML appropriately consider cybersecurity.
- **Cybersecurity Instructions for Continued Airworthiness**: There is currently a lack of standardization on how cybersecurity is included in Instructions for Continued Airworthiness ICA. This poses issues for incorporating Supplemental Type Certificates into aircraft as well as for operators and maintainers to supporting mixed fleets. An ongoing ARC is already considering ICA. It is recommended that the Cybersecurity ARC and ICA ARC collaborate to ensure that cybersecurity is appropriately incorporated into ICA.
- **Cybersecurity and Human Factors**: Human factors is an important consideration in aviation safety. Similarly, it needs to be considered in the realm of cybersecurity. Cybersecurity human factors should include ensuring that personnel are trained to an appropriate level and are able to execute commands, but an additional element is whether language used in relation to cybersecurity may lead to adverse effects. There is an ongoing ARC considering human factors, it is recommended that the Cybersecurity ARC and Human Factors ARC collaborate on an approach to additionally assess how human factors and cybersecurity intersect and where further research is necessary.
- **Decommissioning and disposal of assets:** Decommissioning and disposal of aviation assets, including avionics and ground support equipment, is currently not regulated. Assets may be found on public and uncontrolled platforms or access may be gained through salvage yards. Untrusted actors may be able to obtain or access assets and modify the assets. Such modified assets may than be re-introduced into the supply chain. The ARC should discuss the risk trend in this area and how the industry can protect against such risks.

5.2 Research Supported by AIA

In 2024, the FAA research program known as Information/Cyber Security focused on developing and demonstrating cybersecurity data science (CSDS) concepts that potentially could enhance cybersecurity for the aviation ecosystem. The program is meant to act as a catalyst in utilizing Artificial Intelligence and Machine Learning (AI/ML) on aviation data for cyber security applications in the aviation community. The FAA partnered with Embry-Riddle Aeronautical University (ERAU) and MIT Lincoln Lab to acquire a highly advanced team of subject matter experts in aviation and data science.

The research program emphasized collaboration with the AIA community and other aviation industry stakeholders to address aviation industry key interest areas related to cybersecurity. Some of these areas were Information Security Event Management (ISEM), Aircraft Log Anomaly Detection (ALAD), aviation supply chain vulnerabilities and aviation manufacturing operations.

The ISEM research provided valuable contributions in 2024 to enhance portions of DO-392A/ED-206A. A joint AIA white paper "The Role of Cybersecurity Data Science (CSDS) in Aviation Cybersecurity: Applicability for enhancements to RTCA/EUROCAE standards" was published in 2023 and posted on the AIA website. The CSDS research program has adopted the collaborative research model (shown in the figure below) for the additional key interest areas with research which can support standards development.

ALAD research provided initial insight into the applicability and practicality of using unsupervised machine learning algorithms for the analysis of aircraft logs to identify evidence of cyber-attacks on aircraft systems more quickly and accurately than our current industry analysis processes. These research insights included alteration of our existing OEM and operator log analysis processes and workflows. Early supply chain research identified vulnerability management concepts which can be used to improve the prioritization of existing aviation software patching, reduction of execution time, effort, and associated cost while reducing the risk of threats being introduced through the aviation software supply chain. Manufacturing operations research identified potential data from both manufacturing systems and from product quality sensors that might be used to detect malicious intrusion into factory assembly processes and software.

Demonstrations of prototype capabilities for the key interest areas were developed and provided on a periodic basis to the aviation industry stakeholders. The demonstrations provided a venue for the potential applications of CSDS concepts to various use cases which included input from AIA working group experts. The demonstrations and presentations were also meant to provide a feedback loop to the researchers and provide support to the AIA members in the development of aviation standards.

In 2025, collaborative research will continue to investigate additional industry interests associated with the key interest areas to refine recommendations to our community, while leveraging realistic operational log and manufacturing data generated by simulated aircraft and factory environments. Research results are anticipated to continue informing the enhancement of industry standards, including DO-392A, ARINC-852, ARINC-811, IEC 62443, multiple NIST and ISO documents and others. Results are also expected to inform aircraft operators regarding operating and analysis methods and aviation OEMs regarding manufacturing and systems design, leveraging the benefits of CSDS with AI/ML.

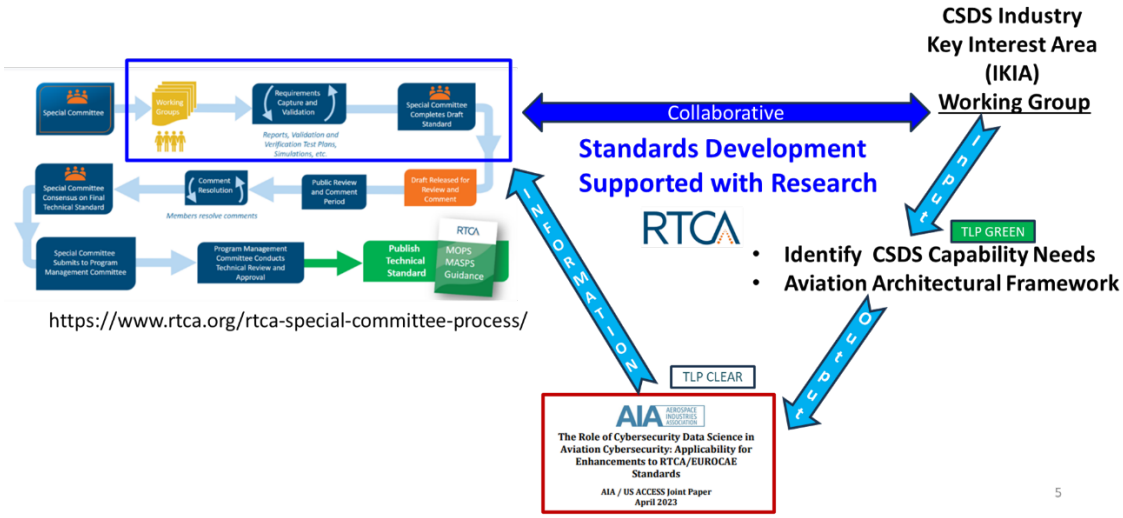

Figure 2: Standards Development Process with AIA/FAA Research Support

The research performed through CSDS and the plans for further work have shown to be extremely beneficial. AIA strongly supports continuation of this research and would propose the research to be expanded. The research conducted by FAA, Embry-Riddle Aeronautical University and MIT Lincoln Labs is of a fundamental nature that benefits the entire sector.

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 Aerospace	Anup Raje	Honeywell
Majed Bouzouita	Boeing	Kanwal Reen	Collins Aerospace
John Bush	Boeing	James Robinson	Boeing
Don Christie	Honeywell	Wes Ryan	Northrup Grumman
Brian Connolly	Boeing	Aneesh Sankruth	Gulfstream
Michael Cook	ATI Metals	Dustin Scheller	Skygrid
Kathleen Finke	Astronautics	Stefan Schwindt	GE Aerospace
Marshall Gladding	Boeing	Sarah Stern	Boeing
Robert Hood	Astronautics	Sean Sullivan	Boeing
Dave Jones	Astronautics	Nora Tgavalekos	RTX
Theodore Kalthoff	Archer	Jason Timm	AIA
Laurel Matthew	Boeing	Jeff Troy	A-ISAC
Steven Marchegiano	ADI American Distributors	Michele Tumminelli	Gulfstream
Tom McGoogan	Boeing	Mike Wiegand	Shift5
Charles Minor	Pratt & Whitney	Mike Vanguardia	Boeing
Alimuddin Mohammad	Boeing	George Vergara	Raytheon

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	NASA
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
Varun Khanna	FAA		