Civil Aviation Cyber Security Annual Report

Given to the AIA Civil Aviation Council
November 2022

Civil Aviation Cybersecurity Subcommittee

Stefan Schwindt – Chair (GE Aerospace)
Sean Sullivan – Vice-Chair (The Boeing Company)
Simone Perez – AIA Leader
Patrick Morrissey – Editor (Collins Aerospace)

Civil Aviation Cybersecurity Industry Assessment & Recommendations
Report to the AIA Civil Aviation Council
November 2022

Contents

1 INTRODUCTION

The AIA Cybersecurity Committee serves the aerospace industry as a community of aircraft manufacturers and their suppliers to promote discussion, define common interest, and advocate for regulatory and standards updates to help ensure the continued safe and secure operation of the industry we serve. To this end, the committee 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 our community as well as a summary of the papers in development and published by the committee in 2022.

2 Regulatory Updates

2.1 U.S.

The FAA is in the process of proposing rulemaking which will include 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 rulemaking is part of the omnibus DRAFT Transport Airplane Certification Modernization Notice of Proposed Rule Making (NPRM) which is going through internal coordination, resolving comments received within the FAA. The NPRM is currently expected to be published in May of 2023 for comment by the

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

public. After receiving and resolving comments, the rule could be published during Q4 of 2024. In the meantime, the FAA has updated Issue Papers to reflect current ASISP trends. This way, all new entrants will reference the latest guidance (DO-326A, DO-355A and DO-356A) while the drafting of the Advisory Circular (AC) is in process. Regulatory Policy and acceptance for Parts 23, 27 and 29 has entered its final stages. Part 23, 27 and 29 are using the F44 ASTM ASISP standard (F3532) as a Means of Compliance (MOC). Both Parts 27 and 29 will be addressing ASISP through the traditional XX.1301 and XX.1309 rules while Part 23 will be addressing ASISP by having applicants step up to amendment 64 rules 23.2500, 23.2505 and 23.2510. There is no plan in the near future for rule making for Part 23, 27 or 29 at the moment.

2.2 E.U.

Part IS, also known as the "horizontal rule" was published as a Delegated Regulation on September 26. This new regulation calls for production and design organizations as well as aerodrome and apron management service providers to establish and maintain an Information Security Management System similar to the Safety Management Systems operated by those organizations. In the near future the scope of Part-IS is planned to grow further to include entities in the remit of the states as Implementing Regulations are adopted (I.e., airlines and other operators, maintenance organizations, air traffic management and air navigation service providers, etc.). Part IS will also apply to the oversight authorities – EASA and the EU National Aviation Authorities. More detailed information can be found at: http://data.europa.eu/eli/reg_del/2022/1645/oj. The EASA ESCP is currently developing the Accepted Means of Compliance & Guidance Material (AMC & GM) to be affiliated with the rule which is effective today with full compliance required by October 16, 2025.

A proposed regulatory framework for the operation of drones was published June 30 under NPA 2022-06. The framework will enable innovative air mobility to address manned VTOL aircraft as well as UAS. In this framework cybersecurity will be addressed in design and operation using the same language defined for other airborne systems through X.1319. AMC 20-42 will serve as the acceptable means of compliance for this segment thus making it a common means for security compliance for all airborne systems. AIA provided formal comments to the NPA earlier this year.

3 Standards Updates

3.1 RTCA SC-216 / EUROCAE WG-72

The RTCA and EUROCAE security committees (SC-216/WG-72) continue to work together on the development of standards material for the industry to ensure common goals and outcomes. The Terms of Reference (TORs) for SC-216 & WG-72 have been revised in 2022 to reflect new work largely driven by ECSCG and US ACCESS WG. Below is the status of the work currently underway by these committees on various standards:

- ED-201A/DO-391 *Aeronautical Information System Security Guidance – published 2021*

  This document provides a framework linking the various security standards for aviation security together to support all stakeholders. This includes aircraft design, production, and operation, as well as air traffic management, airports, maintenance and repair (MROs), aviation services providers, components (SW and HW), and information (such as databases charts and manuals) as well as the supply chains which provide them. This standard includes recommendations on what should be done in addition to current practice. As relevant standards are updated and new ones are generated this standard is also updated to link the appropriate changes. Version "A" was approved by PMC and published December 2021.

- DO-393/ED-205A: *Process Standard Process Standard for Security Certification and Declaration of ATM ANS Ground Systems – published 2022*

  This process standard serves to provide guidance for assessing ground systems are appropriately secured for use in aviation. The proposed process can be used to identify, evaluate, and manage safety as well as non-safety risks. The updated version is meant to be in line with the new EU basic regulation and Part IS, as such, it could serve as an AMC for the aforementioned regulation. DO-393/ED-205A was published mid-2022.

- DO-392/ED-206: *Security Event Management and Continued Airworthiness – published 2022*

  DO-392/ED-206 is projected to be an important standard in aviation once released as it impacts all stakeholders in the aviation ecosystem. It will form part of the AMC/GM to EASA's Part IS on incident and vulnerability management. It is also anticipated that the FAA may use it for cyber related aspects of occurrence reporting. As we (AIA) anticipate the document will be used in US and EU contexts, many AIA members have participated on behalf of their organizations to help ensure the standard can be applied with consistency in both jurisdictions setting common expectations and a level playing field. The following items are considered important elements of the standard for inclusion:

  1. Performance requirements for detecting and identifying security events and determining if they are security incidents
  2. Performance requirements for detecting and identifying vulnerabilities
  3. Thresholds for reporting incidents up to TC Holders and/or authorities
  4. Thresholds for reporting vulnerabilities up to TC Holders and/or authorities
  5. Allowable timetables for mitigating and/or fixing vulnerabilities dependent on criticalities
  6. Allowable timetables for responding to incidents and securing/restoring systems
  7. Patching vs. reporting (i.e. if patching is fast enough is reporting required?)

  Additionally, once the document is released it will be up to the member organizations adopt the standard in their supplier contracts to ensure consistency in addressing incidents and vulnerabilities that can affect aviation safety throughout the entire supply chain. This standard was published mid-2022.

- DO-326B/ED-202B *Airworthiness Security Process Specification*

  The DO-326B revision will include guidance on Security Change Impact Analysis. The AIA recommendations paper on Security Change Impact Analysis will help drive the direction of this revision.

- DO-ISMS/ED-ISMS *Information Security Management System Guidance*

  This new joint document will provide guidance on how to set up an Information Security Management System (ISMS) within aviation and serve as guidance material to the recently published EASA Part-IS. It will leverage best practices from Safety Management System (SMS) as appropriate.

- DO-392A/ED-206A *Security Event Management and Continued Airworthiness*

  This recently published standard will be revised to address performance requirements for event reporting and close out non-concur comments from the last FRAC/OC.

- DO-DSEC/ED-DSEC *Aviation Data Security*
  This new joint document is still being scoped, but it may include dataload, distribution, maintenance data, data storage, target software storage, maintenance data, etc. This document will provide objectives for securing relevant data at rest and in transit.

3.2 SAE G-32 Cyber Physical System Security

SAE G-32 is divided into the following subgroups and corresponding documents:

- JA7496 Cyber Physical Systems Security Engineering Plan document has been released June 2022.
- CPSS Software Assurance (JA6678) preparing draft. They are also planning to generate cybersecurity guidance starting 2023 that SAE G-34 / EUROCAE WG-114 AI/ML in Aviation can reference.
- CPSS Hardware Assurance (JA6801) preparing draft

3.3 SAE E-36

With the expectation for the FAA to update Parts 33 & 35 (engines and propellers) to include cybersecurity design requirements (xx.1319) the Electronic Engine Controls Committee (E-36) is developing AIR7368 *Cybersecurity for Propulsion Systems*. This document will provide guidance for engine and propeller control systems certification for Cybersecurity. The E-36 committee is being supported by attendees from regulators and propulsion manufactures as well as OEMs in support of integration.

A draft is currently available for review with final ballot is expected in January 2023 after the E-36 plenary.

3.4 Internet Protocol Suite (IPS)

Aeronautical Telecommunications Network over Internet Protocol Suite is Next Gen protocols for air-to-ground safety communications to support multiple access sub-networks. Industry activity spans four standards bodies:

- ARINC EEC IPS Subcommittee
- RTCA SC-223 / EUROCAE WG-108
  - Actively working revisions to Fail Secure/Degraded Modes section of MASPS
- ICAO Aeronautical Communication Panel - Data Communication Infrastructure Working Group I
  - IPS SARPS (Standards and Recommended Practices Report) review planned for Oct 2022 submission for comments (like FRAC)
  - DOC 9896 “Manual for the Aeronautical Telecommunication Network (ATN) using IPS Standards Ed.3” planned for Oct 2022 submission for comments (like FRAC)
  - IPS deployment pushed out 2 years to the end of 2024, now better aligned with new apps & datalinks being developed and deployed by System Wide Information Management (SWIM) & Single European Sky ATM Research (SESAR)
  - IPS Security Subgroup working requirements for network/layer-3 security (end-2-end), capable of using multiple datalinks concurrently
  - Trust Framework Study Group and Secretariat Study Group on Cybersecurity (SSGC) promoted to Panel

3.5 Unmanned Aircraft Systems (UAS) Standards

RTCA SC 228/EUROCAE WG 105, approval for publication of the documents by RTCA PMC September 15

- DO 365C Minimum Operational Performance Standards (MOPS) for Detect

- and Avoid (DAA) Systems
- DO 397 Guidance Material: Navigation Gaps for Unmanned Aircraft Systems
- DO 398 DAA Operational Services and Environment Definitions (OSED)

AIA Advanced Airborne Mobility (AAM) Subcommittee is adding cyber inputs to their AAM Privacy Work Group paper.

3.6 Other Cyber-Related Standards

SC-236 / WG-96 Wireless Avionics Intra Communication System (WAIC) is working on MOPS and planning to consult SC-216 / WG-72 for cybersecurity requirements. The committees agreed to only include minimum requirements necessary for supplier to create device via TSO. There will be two TSOs resulting from the MOPS: one for the WAIC radio and one for "Full Security Device" Gateway functions. This will allow simple sensors and more complex devices to be developed independently. SC-236 / WG-96 Working Group 1 is focused on the frequency / spectrum requirements, while 2, 3, & 4 focus on the rest (to include security).

ARINC AEEC NIS has a new work statement to include a revision to ARINC 811 Commercial Aircraft Information Security Concepts of Operation and Process Framework.

3.7 Standards Coordination

European Cybersecurity Standards Coordination Group (ECSCG) Rolling Development Plan V4.0 has been released: https://ecscg.eu/media/1249/ecscg-c-rdp-v40.pdf. The ACI US Aviation Coordination of Cybersecurity & E-enabled Standards Strategy (US ACCESS) Working Group has been focusing on the US only delta to include standards used by the US military. They have been fostering the harmonization of EU/US standards in eVTOL (Vertical Take Off and Landing). There a plans for a joint AIA and US ACCESS recommendations paper on Cyber Security Data Science (CSDS) in 2023.

Both standards coordination groups have provided input to the SC-216 / WG-72 TOR, and representatives from both standards coordination groups have presented their work at the A-ISAC ACI Annual Summit. The presentation raised awareness of both coordination groups and the successes to date. As a result, several new volunteers for US Access have come forward.

4 AIA Recommendation Papers

Below is a summary of the papers developed this year by the AIA Cybersecurity Committee and those which are still in development (to be completed in 2023).

4.1 ALPA / AIA Joint Recommendations

This paper summarizes discussions hosted in 2021 between pilots, represented by ALPA, and airplane and avionics system manufacturers, represented by the Aerospace Industries Association (AIA) Civil Aviation Cybersecurity Subcommittee. The paper provides an overview of topics which were covered in those discussions and the conclusions which were drawn. Many of the topics resulted in considerations for future research activities, design, and process updates. The focus of the discussions was cybersecurity risks, mitigations, and if/how pilots might need to be informed of, or respond to, those events. This in turn raised questions about how the pilot receives, interprets, and uses data from the modern connected aircraft. As with any potential safety impacting event on an aircraft, mitigations to prevent their occurrence can be technical (i.e., handled by the aircraft and its systems), procedural (i.e., requiring pilot notification, intervention, and training), or physical (e.g., cockpit security door).

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

4.2 Software Security

Efforts to enhance secure software distribution and secure software loading practices throughout aviation ecosystem are ongoing. Significant strides have been taken in establishing standards and various implementation methodologies have been provided to the industry to help advance secure software distribution and loading in the aviation domain. This paper seeks to provide guidance for compliance to new aviation standards and provides recommendations to standardize best practices as much as possible. This guidance complements the 2020 software recommendation paper establishing the basis for ARINC 645-1 secure dataloaders and provides proposals for transitioning civil aviation to secure software distribution for all aircraft. Suggested timeframes for adhering to each phase are also provided.

4.3 Change Impact Analysis for Major/Minor Determinations

The committee started development of a whitepaper intended to cover how cybersecurity impacts are identified as part of the product change classification under 21.91 and 21.101. An update to this process would enable the industry to identify changes at the system, software, or hardware level, and what amount of verification or reverification is needed to address aircraft and system security where security is a driver for the major/significant or major/non-significant change. Based on engagement with SC-216 / WG-72, the recommendations to update RTCA DO-326A/ED202A have been accepted. The draft whitepaper material seeks to provide guidance for compliance to new aviation standards and provide recommendations to standardize best practices as much as possible. As SC-216 / WG-72 has accepted the recommendation to update DO-326A/ED-202A in accordance with AIA's intent, the activities on the whitepaper are transitioning formally to SC-216/WG_72 to be adopted in the updated standard. AIA's problem statement and expectations are documented to ensure appropriate update of the standard.

Appendix A: Members & Contributors

AIA Working Group Members

Mayank Agarwal	Infosys	Steven Marchegiano	ADI American Distributors
Ruchik Amin	GE Aviation	Tom McGoogan	Boeing
David Almeida	LS Technologies	Alimuddin Mohammad	Boeing
Steve Benham	GE Aviation	Patrick Morrissey	Collins Aerospace
Majed Bouzouita	Boeing	Siobvan Nyikos	Boeing
John Bush	Boeing	Suzanne Patterson	Boeing
Don Christie	Honeywell	Kanwal Reen	Collins Aerospace
Brian Connolly	Boeing	James Robinson	Boeing
Michael Cook	ATI Metals	Stefan Schwindt	GE Aviation
Kathleen Finke	Astronautics	Sarah Stern	Boeing

Marshall Gladding	Boeing	Sean Sullivan	Boeing
Todd Gould	Boeing	Amir Taheri	Pratt & Whitney
Dave Jones	Astronautics	Nora Tgavalekos	Raytheon Technologies
Bret G Lynch	Pratt & Whitney	Jason Timm	AIA
Laurel Matthew	Boeing	Jeff Troy	A-ISAC

Cyber Working Group Guests/Observers:

Diessner, Daniel J	Embry Riddle	Samantha Lopresti	FAA
Gabe Elkin	MIT Lincoln Lab	Paul Nelson	NASA
Will Gonzalez	FAA	Steve Ramdeen	FAA
Sidd Gejji	FAA ACI Tri Chair	Ted Rush	FAA
Jerry Hancock	Inmarsat / ASD	Julien Touzeau	Airbus
Theodore Kalthoff	Bombardier	Isidore Venetos	FAA
Terry Kirk	Aviation ISAC	Philip Windust	FAA
Varun Khanna	FAA	Hank Wynsma	United Airlines