Civil Aviation Cyber Security Annual Report

Given to the AIA Civil Aviation Council November 2023

Civil Aviation Cybersecurity Subcommittee

Stefan Schwindt – Chair (GE Aerospace)
Sean Sullivan – Vice-Chair (The Boeing Company)
Chad Kirk – AIA Senior Director
Patrick Morrissey – Editor (Collins Aerospace)

Contents

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

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 2023.

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 NPRM is currently expected to be published Q1 2024 for comment by the public. After receiving and resolving comments, the rule could be published during Q4 2024 / Q1 2025. In the meantime, the FAA has updated issue papers to reflect current ASISP trends. The Advisory Circular (AC) will be published concurrently with the rule and provide the Accepted Means of Compliance (AMC), referring to the industry standards generated by RTCA SC-216 and EUROCAE WG-72. Part 23, 27 and 29 will be expected to use the F44 ASTM ASISP standard (F3532) as a Means of Compliance (MOC) after an update is published in 2024. 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.

In March 2023, the TSA released the same reporting measures proposed last summer in the form of an Emergency Amendment, impacting airports and operators.

CISA developed "Cross-Sector Cybersecurity Performance Goals (CPGs)" and future development of transportation-specific performance goals (Link).

Toward the end of 2023, there has been an uptick of RFIs from the executive branch regarding cybersecurity. AIA has responded to the Office of the National Cyber Director (ONCD) RFI and is engaging in continuing discussion on how to manage regulatory workload from cybersecurity requirements derived from multiple agencies.

2.2 E.U.

Part-IS, also known as the "ISMS rule" was published through two legal acts a Delegated Regulation on September 26, 2022, and an Implementing Regulation on February 2, 2023. This new regulation calls for aviation organizations and EU competent authorities for aviation, including EASA, to establish and maintain an Information Security Management System similar to the Safety Management Systems operated by those organizations. The rule is effective today with full compliance required by October 16, 2025 for organizations in the scope of the Delegated Regulation and by February 22, 2026 for the other organization and authorities in the scope of the Implementing Regulation. More detailed information can be found at: Implementing Regulation, and Delegated Regulation. EASA and the European Strategic Coordination Platform (ESCP) have developed the Acceptable Means of Compliance & Guidance Material (AMC & GM) to be affiliated with the rule and this material has been published on July 13, 2023.

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 and WG-72 were revised in 2022 to reflect new work largely driven by the European Cyber security for aviation Standards Coordination Group (ECSCG) and the Aviation Cybersecurity Initiative (ACI) US Aviation Coordination of Cybersecurity & E-enabled Standards Strategy (US ACCESS) WG. Below is the status of standards in work by these committees for the SC-216 Terms of Reference and WG-72 Task Sheet:

- 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 was started to drive the direction of this revision, and then work was transferred to SC-216/WG-72. This document will enter Final Review and Comment / Open Comment January of 2024 with an expected publication date in June 2024.

- DO-ISMS/ED-ISMS *Information Security Management System Guidance for Aviation Organizations*

  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 and supplement Safety Management System (SMS) as appropriate.

- DO-392A/ED-206A *Guidance on Security Event Management*

  This standard, last published in 2022, 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 *Standards on Aviation Data Security*

  This new joint document includes guidance for secure 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.

During discussions within the AIA Cybersecurity Subcommittee, issues with interpretation of DO356A in various certification projects have been identified which are causing impacts on cost and scheduling for applicants. These issues have been collated and the TOR for SC-216 are being revised to plan a DO356A Change 1 document and a new report to find resolutions for these issues.

3.2 RTCA SC-223 / EUROCAE WG-108

The RTCA and EUROCAE security committees (SC-223/WG-108) continue to work together on the development of standards material for the industry to ensure common goals and outcomes. The Terms of Reference (TOR) for SC-223 & WG-108 were revised for Version 9, in September 2023 to reflect new work to update the certification technical profiles for several IETF RFC protocol standards related to secure communication and PKI.

- DO-404/ED-315 *"Minimum Aviation System Performance Standards (MASPS) on ATN/IPS End-to-End Interoperability and Certification."*

This recently released (September 2023) joint document provides the certification and end-to-end interoperability requirements that include the safety and security considerations for air and ground IPS subsystems. The MASPS go into the details of the IPS Security architecture of the secure communication channels between Air Navigation Security Providers, Airline Aeronautical Operational Control, and the aircraft that protect the datalink data plane. This also includes controls to protect the IPS control plane between aircraft and communication service providers.

- DO-379A/DO-262A *"Technical Standard of Aviation Profiles for Internet Protocol Suite"*

  The IPS profiles document the unique adaptations required to enable current Internet Engineering Teak Force (IETF) Request For Comment (RFC) documents to specify the technical requirements for Aeronautical data communications between an aircraft system and its corresponding peer on the ground. There is a heavy focus on requirements to secure the IPv6 network traffic leveraging Datagram Transport Layer Security and Public Key Infrastructure (PKI).

3.3 RTCA SC-214 / EUROCAE WG-92

RTCA SC-214 is a joint committee with EUROCAE WG-92 working in collaboration with AEEC Data Link (DLK) Systems Subcommittee to ensure harmony within VDL Mode 2 standards. The Terms of Reference (TOR) for SC-214 & WG-108 were revised for Version 9, in September 2023 to reflect new work to update VDLm2 standards to support data communications over the new ATN-IPS network being developed by SC-223/WG-108 and incorporate derived requirements account for secure transport and integrity controls.

- DO-224E *"Signal-in-Space Minimum Aviation System Performance Standards (MASPS) for Advanced VHF Digital Data Communications"* is defining the requirements to support ATN/IPS via a subnetwork adaptation to convey the IPv6 frames over VDL Mode 2. A new adaptation layer named IPS Over AVLC (IOA) has been defined. The IOA Protocol will make VDLm2 IPS-Capable and provides the layered security controls needed to protect the integrity of ATC traffic for safety services.

3.4 SAE G-32 Cyber Physical System Security

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

- Cyber Physical Systems Security Engineering Plan (JA7496) has been released June 2022 and work continues on the development of Revision A.
- CPSS Software Assurance (JA6678) has completed two ballot rounds.
- CPSS Hardware Assurance (JA6801) has prepared a draft version.

3.5 SAE E-36

With the expectation for the FAA to update Parts 33 & 35 (engines and propellers) to include cybersecurity design requirements (corresponding to 25.1319 for large aircraft) the Electronic Engine Controls Committee (E-36) published AIR7368 *Cybersecurity for Propulsion Systems* September 2023. 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.

3.6 AEEC IPS Subcommittee

The Internet Protocol Suite (IPS) for Aeronautical Safety Services Subcommittee leads the standardization effort to provide ATN/IPS safety services to the aircraft. It is defining the transition path from ACARS and ATN/OSI

services to ATN/IPS. ARINC 858 provides the technical requirements, to include security provisions to allow existing ATC and AOC applications to securely communicate over an IP link.

- Draft 2 of Supplement 1 to ARINC Specification 858P1, *"Internet Protocol Suite (IPS) For Aeronautical Safety Services Part 1 Airborne IPS System Technical Requirements"*

  With the move to an IP protocol stack the airborne technical requirements include several security provisions and requirements that define the security architecture, security mechanisms, and security support functions such as key management and security event logging, informed by other security-oriented technical standards like ARINC 842 and DO-356A, and security design and implementation guidance.

- Draft 2 of Supplement 1 to ARINC Specification 858P2, *"Internet Protocol Suite (IPS) For Aeronautical Safety Services Part 2 IPS Gateway Air-Ground Interoperability"*

  As a part of the layered IPS security approach, each air-ground access network must be secured. Authentication for IPS service must be supported across all air-to-ground links. This specification describes how authentication is performed between the Airborne IPS System and the communicating peer Ground IPS System (i.e., IPS Gateway or Ground IPS Host), the placement of which is dependent on the deployment option.

- Draft 2 of ARINC Project Paper 858P3, "*Internet Protocol Suite (IPS) for Aeronautical Safety Services, Part 3, Common IPS Radio Interface (CIRI)"*

  The Common IPS Radio Interface (CIRI) protocol specified in Part 3 is intended to provide a datalink adaptation function to accommodate radio-specific interfaces. This enables different radios to handle information.

3.7 ICAO Communication Panel

With the increasing reliance on automated systems and networked communications, protection from malicious, intentional, and unintentional interference is needed to ensure the safety and integrity of the global Air Traffic Management (ATM) system. The ICAO CP is working to modernize the communication technology stack used to support aeronautical communication between aircraft and Air Navigation Service Providers. This work is focused out of the Data Communication Infrastructure Working Group (DCIWG) and Working Group I and involves the update and creation of IPS Standards and Recommended Practices (SARPS), supporting Manuals, and Guidance material on Air Navigation (Cyber) Resilience. Standards currently in development include the following:

- Annex 10 — *Aeronautical Telecommunications, Volume III — Communication Systems, Part I — Digital Data Communication Systems* and *Volume II — Communication Procedures including those with PANS status*.

  A Proposal for Amendment (pfA) to amend Annex 10 has been authorized by the ICAO Commission and transmitted to Member States and appropriate international organizations for comments on 31 July 2023. The proposal introduces provisions relating to updates to the aeronautical telecommunication network (ATN)/Internet Protocol Suite (IPS) requirements regarding IPS mobility, naming and addressing, security, and other transitional aspects.

- Doc 9896 Ed 3. *"Manual for the Aeronautical Telecommunication Network (ATN) using IPS Standards"*

  Edition 3 of the manual contains the minimum communication standards and protocols that will enable implementation of an ICAO aeronautical telecommunication network (ATN) based on the Internet protocol suite (IPS), referred to as the ATN/IPS. The scope of this manual is on

interoperability across administrative domains and includes all of the performance, security, and general technical requirements associated with implementing IPS.

- Doc 10090 *"Manual of Security Services for Aeronautical Communications"*

  This manual provides information about the security services and technology stacks embedded throughout of the ATN/IPS system, to include guidance on their use and implementation. It is meant to assist implementers and users of the ATN/IPS to ensure interoperable, safe, and secure, services. Note that an attempt has been made to harmonize with the "*Manual of Information Security*" being developed under the ICAO Trust Framework Panel.

- Doc 10095 *"Manual of the Public Key Infrastructure (PKI) Policy for Aeronautical Communications"*

  The ATN/IPS design includes security measures to protect the exchange of digital data and the participating subsystems. This manual provides information on how to manage the digital certificates used by ATN/IPS. Note that an attempt has been made to harmonize with Doc 10169 "*Manual of Aviation Common Certificate Profile (ACCP)*" being developed under the ICAO Trust Framework Panel.

- Doc 10145 *"Manual of Security Risk Assessment for Aeronautical Communications"*

  This manual provides a generic Security Risk Assessment (SRA) of an IPS system within the context of the Air Traffic Services (ATS) data link and Aeronautical Operational Control (AOC) safety data communications. The IPS airworthiness security risk assessment was developed in accordance with the emerging airworthiness security regulations and defined in DO-326A/ED-202A, DO-356A/ED-203A, and DO-393/ED-205A. It informs IPS manufacturers, operators, and certifiers on their IPS product and service-specific risk assessments.

3.8 ICAO Trust Framework Panel (TFP)

The evolution of systems for data and information processing raised concerns in the aviation community regarding the effectiveness of existing standards, procedures, and processes to ensure the risks involved in the exchange of messages in a digital environment are kept at an acceptable level. The TFP is charted to develop, address, and maintain provisions and guidance materials to support globally harmonized frameworks enabling the trusted exchange of data and information amongst states, relevant stakeholders, airspace users, service providers and new entrants. The TFP is currently working to release three new ICAO Docs:

- Doc XXX *"Manual for Information Security"**
- Doc 10169 *"Manual for an Aviation Common Certificate Profile"*
- Doc XXX *"Guidance on Implementing Digital Identities"**

**these documents are in development and only have provisional placeholders.*

3.9 ICAO Cybersecurity Panel (CYSECP)

A new ICAO Panel for Civil Aviation Cybersecurity has recently been stood up with the objective of developing Standards and Recommended Practices (SARPs), procedures and guidance material for safeguarding civil aviation against cyber threats. The Terms of Reference states the CYSECP has the following statement of work:

- Conduct periodic reviews of the ICAO Aviation Cybersecurity Strategy and Action Plan.
- Assess and report on the evolution of aviation cybersecurity threats and risks.
- Development of guidance material and technical requirements related to aviation cybersecurity.

There are currently two new Working Groups to develop aviation cybersecurity guidance:

- WGCTR – Working Group on Cyber Threats and Risks
- WGCGM – Working Group on Cyber Guidance Material

3.10 ICAO Navigation Systems Panel (NSP)

The NSPs main task is to develop ICAO SARPs and guidance material for air navigation systems. NSP activities in the cybersecurity field are limited to aspects directly relevant to navigation systems used to support civil aviation. Apart from ground systems and interfaces, cybersecurity threats are scoped to "cyber-over-RF" attacks targeting avionics and aircraft. Significant NSP cyber activity is underway to develop Space Based Augmentation Systems (SBAS) authentication to provide protection against Global Navigation Satellite Systems (GNSS) Radio Frequency Interference (RFI) / Spoofing.

3.11 Unmanned Aircraft Systems (UAS) Standards

RTCA SC-228/EUROCAE WG-105, approved the following documents for publication by RTCA PMC on September 15, 2023:

- 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 added cyber inputs to their AAM Privacy Work Group paper. The AIA UAS Data Protection Community of Interest, which is a working group within the AIA, has a draft appendix for NAS 9948 titled "Test Procedures for NIST 800-53 Rev. 5 Security and Privacy Controls."

AI/ML is an enabler for UAS and was a topic of interest at the Aviation Cybersecurity Summit 2023. AI/ML industry activity includes:

- SAE G-34/WG-114 AI/ML in Aviation Committee: AIR6987 Artificial Intelligence in Aeronautical Systems: Taxonomy in balloting process.
- RTCA hosted an AI/ML Workshop in November.
- EASA published Artificial Intelligence concept paper and roadmap.

3.12 Other Cyber-Related Standards

SC-236 / WG-96 Wireless Avionics Intra Communication System (WAIC) is closing out FRAC comments for their Minimum Operational Performance Standard (MOPS) having previously consulted with SC-216 / WG-72 for cybersecurity requirements. The committees agreed to only include minimum requirements necessary for suppliers to create devices 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:

- Revision to ARINC 811 Commercial Aircraft Information Security Concepts of Operation and Process Framework. The focus will be how to do a threat assessment from the perspective of an operator.
- Revision to ARINC 822 which will focus on Wi-Fi and Cellular links.

Related to ARINC AEEC NIS, ARINC Next Generation Network Technology for Avionics Communication (NTAC) Subcommittee is generating two new ARINC Project Initiation/Modification (APIM) with cyber impact:

- Ethernet-compatible Field Bus for Airborne Communication Platforms.
- Next Generation Network Technology for Avionics Communications.

ARINC is also establishing a new AEEC Operator-Focused Cybersecurity Users Forum.

SAE S-18 Aircraft and Sys Dev and Safety Assessment Committee 2023 activities include:

- SAE S-18 & EUROCAE WG-63 now have formal liaison with SC-216/WG-72.
- ARP4761A Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment approved by Aerospace Council for publication.
- ARP4754B Guidelines for Development of Civil Aircraft and Systems approved by the Aerospace Council for publication.

For software security, ARINC 827, 835, 645-1 are being reworked (software security, secure data loading related). The Digital Security Working Group (DSWG) is working an update to ATA Spec 42.

3.13 Standards Coordination

European Cybersecurity Standards Coordination Group (ECSCG) Rolling Development Plan V4.0 has been released (Link). 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. The joint AIA and US ACCESS recommendations paper on Cyber Security Data Science (CSDS) has been published with planned incremental revisions. It has been socialized with SC-216 to advise and provide input for the ED-206/DO-392 revision.

3.14 A-ISAC

While not a standards organization, it is worth mentioning the Aviation Information Sharing and Analysis Center (A-ISAC). The A-ISAC had its quarterly AvTech events plus its annual Aviation Cybersecurity Summit in Dublin, Ireland September 2023. Common themes included AI/ML, model-based engineering, secure design and test, and GNSS RFI/spoofing and jamming. The next summit will be September 17-19, 2024, in New Orleans, Louisiana.

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 Need for Considering Security of Artificial Intelligence and Machine Learning in Aviation

With the 2023 release of several Artificial Intelligence/Machine Learning (AI/ML) applications, there has been a heightened interest across all industrial sectors in using these new tools. The promise of AI/ML is to automate many tasks that previously were only achievable manually through humans as well as unlock new capabilities by utilizing many large and different data sources. However, the use of AI/ML introduces new threats as evident in existing applications. As a safety-critical industry with long lifecycles and slow rate of change, AI/ML should only be deployed with appropriate safeguards. While Standards Development Organizations are developing standards for implementing AI/ML with protections against unintentional errors, the current work is not considering protections against intentional errors and attacks on AI/ML. It is considered imperative that the

relevant working groups include cybersecurity considerations so that the first issue of the AI/ML certification standards may allow approval of AI/ML in aviation for a safe and secure implementation and deployment.

4.2 Recommendations on the Use of Software Bill of Materials in Aviation

SBoMs provide a mechanism for transparency of the supply chain, so that the parties who use, produce, and operate software with 3rd party components have a better understanding of the supply chain associated with the components. This has the added advantage by helping bring understanding to the cyber risk associated with the 3rd party software components being used, and potential to assess the impact of known and newly emerging vulnerabilities. The aviation industry should encourage the generation and maintenance of SBoMs for aircraft systems, due to the benefit that they provide in areas of vulnerability management, assessing technical debt, besides understanding the complex software supply chain.

AIA recommends that the appropriate regulations be updated to encourage the generation and maintenance of SBoMs as a part of the software configuration management processes and require the organizations in the aviation ecosystem to implement vulnerability management processes that use SBoMs to detect and analyze vulnerabilities in a timely manner. Since the risk assessment to understand the exploitability and impacts of a given vulnerability in a system might require implementation-level knowledge, it is recommended that the assessment be done by the producers of the software, and delivery of SBoMs to the TC holder and operator or end user not be mandated. This would also require the industry to establish common benchmarks/ thresholds for performing risk assessment and a common taxonomy to communicate the information across different tiers in the aviation ecosystem.

4.3 Civil Aviation Supply Chain Cybersecurity Recommendations Report

Since the original version of this paper new legislation and standards have been released, and the level of attention and consideration for supply chain threats continues to grow. This update is focused on bringing the white paper up to date with the current state of the art in a moment when attention on the topic is at an all-time high. The paper has been restructured, simplified, and rationalized. The updates include consideration of the two new executive orders 14014, “America’s Supply Chains” and 14028, “Improving the Nation’s Cybersecurity,” and standards references have been updated. The NIST 800-161 rev 1 has been considered on how to manage risk. The impact of SBOM (Software Bill of Materials) is discussed and contextualized in the various aviation domains. A link with Part-IS has been added and the paper now identifies a more comprehensive set of threats to the civil aviation supply chain, such as HW vulnerabilities, vetting of suppliers, and other use cases.

Appendix A: Members & Contributors

AIA Working Group Members

Alimuddin Mohammad	Boeing	Laurel Matthew	Boeing
Amir Taheri	Pratt & Whitney	Majed Bouzouita	Boeing
Aneesh Sankruth	Gulfstream	Marshall Gladding	Boeing
Anup Raje	Honeywell	Mayank Agarwal	Infosys
Bret G Lynch	Pratt & Whitney	Michael Cook	ATI Metals
Brian Connolly	Boeing	Mike Tumminelli	Gulfstream
Chad Kirk	AIA	Mike Vanguardia	Boeing
Damani Corbin	Boeing	Nora Tgavalekos	UTC

Dave Jones	Astronautics	Patrick Morrissey	Rockwell Collins
David Almeida	LS Technologies	Ruchik Amin	GE Aerospace
Don Christie	Honeywell	Sarah Stern	Boeing
Robert Hood	Astronautics	Sean Sullivan	Boeing
James Robinson	Boeing	Siobvan Nyikos	Boeing
Jason Timm	AIA	Stefan Schwindt	GE Aerospace
Jeff Troy	A-ISAC	Steve Benham	GE Aerospace
John Bush	Boeing	Steven Marchegiano	ADI
Kanwal Reen	Collins	Theodore Kalthoff	Archer
Kathleen Finke	Astronautics	Tom McGoogan	Boeing

Cyber Working Group Guests/Observers:Cyber Working Group Guests/Observers:

Jeffrey Burkey	FAA	Randy Talley	ACI Tri Chair
Stephane Chopart	Airbus	Sam Masri	Honeywell
Denise Hampt	AirForce	Samantha Lopresti	FAA
Daniel J Diessner	ERAU	Sidd Gejji	FAA
Gabe Elkin	MIT LL	Steve Ramdeen	FAA
Garfield, Keith	ERAU	Ted Rush	FAA
Hank Wynsma	United Airlines	Terry Kirk	A-ISAC
David P Harvie	ERAU	Theodore Kalthoff	Bombardier
Isidore Venetos	FAA	Thomas Parmer	FAA
Clifford Jayson	ERAU	Varun Khanna	FAA
Jerry Hancock	Inmarsat	Vincent A Varouh	NASA
Gernot Ladstaetter	Airbus	Vitaly Guzvhva	ERAU
Paul Nelson	NASA	Lauren N Warner	ERAU