Civil Aviation Cyber Security Annual Report

Given to the AIA Civil Aviation Council
December 2021

Civil Aviation Cybersecurity Subcommittee

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

Civil Aviation Cybersecurity Industry Assessment & Recommendations
Report to the AIA Civil Aviation Council
September 2020

Contents

1 INTRODUCTION

The AIA Cybersecurity Committee serves the aerospace industry as a community of aircraft manufacturers 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 regulator updates which are important to our community as well as a summary of the papers in development and published by the committee in 2021. The following papers were published by the committee in 2021:

- AIA Position on Cybersecurity Testing (Sec 5.3)

For 2022, the committee will continue to work on the open topics listed below as well as advocate for a new potential standard as an outcome of the published cybersecurity testing paper.

  - Papers in development:
  - AIA / ALPA Joint Recommendations, planned Q1 2022
  - Software Security (further guidance planned Q2 2022)
  - Change Impact Analysis, planned Q4 2022
  - Supply Chain (further guidance planned Q4 2022)
- New Topics:
  - Aircraft Security Log File Management and Handling
  - AIA Response to Executive Orders

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

2 Regulatory Updates

2.1 U.S.

The FAA is in the process of proposing rulemaking for Part 25 category aircraft as well as parts 33 engines and 35 propellers. The DRAFT Transport Airplane Certification Modernization NPRM 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 public. After receiving and resolving comments, the rule likely to be published July of 2024. In the meantime, the FAA may update current Special Condition Issue Papers to reflect acceptance of RTCA guidance DO-326A, DO-355A, and DO-356A as an acceptable means of compliance (MOC) until the formal rules are published with these standards as the Acceptable Means of Compliance (AMC). Future plans for Parts 23, 27 and 29 involve using the F44 ASTM standards as a MOC for Cybersecurity. Both Parts 27 and 29 will be addressing Cybersecurity through the traditional XX.1301 and XX.1309 rules while Part 23 will be addressing Cybersecurity by having all applicants utilize amendment 64 rules 23.2500, 23.2505 and 23.2510.

As a result of various supply chain attacks outside of aviation in 2020, several Executive Orders have been released aimed to strengthen supply chains in general and also in particular for critical infrastructures. A National Security Memorandum discusses improving Cybersecurity for Critical Infrastructure Control Systems. The following Executive Orders may become relevant to the aviation industry through direct application or by providing standards usable to aviation:

Executive Order	Title	Link
EO 14036	Promoting Competition in the American Economy	https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/
EO 14034	Protecting Americans' Sensitive Data from Foreign Adversaries	https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries
EO 14028	Improving the Nation's Cybersecurity	https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
EO 14017	America's Supply Chains	https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains
EO 14005	Ensuring the Future Is Made in All of America by All of America's Workers	https://www.federalregister.gov/documents/2021/01/28/2021-02038/ensuring-the-future-is-made-in-all-of-america-by-all-of-americas-workers

Bills on cybersecurity and supply chain have been proposed in both houses of the United States Congress.

2.2 E.U.

For aircraft, EASA has published Aircraft Cybersecurity rules applicable to all certification specifications via ED 2020/006/R. The rules introduced into CS-23, CS-25, CS-27, CS-29, CS-E, CS-P, CS-APU and CS-ETSO entered into force January 2021. For all aircraft parts and products, the common AMC 20-42 references the industry standards ED-202A (DO-326A), ED-203A (DO-356A) and ED-204A (DO-355A) as AMC.

Beyond the aircraft itself, EASA is developing rules to secure the aviation ecosystem using the proposed Part IS. This "horizontal cybersecurity rule" introduces cybersecurity requirements for organizations to implement information security management systems. EASA published Opinion 03/2021 "Management of Information Security Risks" https://www.easa.europa.eu/document-library/opinions/opinion-032021 detailing the proposed rule. The European Strategic Coordination Platform (ESCP) was formed to support this rulemaking task and is currently working on the finalization of the AMC and Guidance Material (GM) to support the future Part IS. Part IS is currently in the "trilogue" phase for negotiation by the European Commission, European Parliament and European Council for final adoption as a regulation. The expected completion of the trilogue is the second half of 2022.

The EU is also in the process of updating their critical infrastructure regulation – the Network and Information Security (NIS) Directive. This proposed update – referred to as NIS 2- includes provisions for including manufacturers of aerospace components as "Important Entities". The European aviation industry has produced a position paper https://www.asd-europe.org/sites/default/files/atoms/files/ASD%20Position%20Paper%20-%20NIS%20Directive%20Final%20%20Submited.pdf on the impact these proposals will have on the manufacturing industry. The NIS 2 proposal is also currently in the trilogue phase and also expected to complete in the second half of 2022.

3 Standards Updates

3.1 RTCA / EUROCAE

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 TORs for SC-216 & WG-72 are expected to be revised in 2022 to reflect new work largely driven by ECSCG. Below is the status of the work currently underway by these committees on various standards:

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

  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" is expected to be 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*

  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 AISS, as such, it could serve as an AMC for the aforementioned regulation.

The SC-216 and WG-72 working groups have completed the proposed standard and are making it available for Final Review and Comment (FRAC)/Open Consultation (OC). Comments are needed by 5:00 PM EST Thursday, January 13, 2022. The comments will be addressed at the next plenary session. Note that editorial, reference numbers, and format/style issues will be resolved as part of the FRAC process.

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

  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. FRAC/OC closed December 13, 2021.

3.2 ARINC 645-1

ARINC 645-1: Common Terminology and Functions for Software Distribution and Loading was approved by AEEC and published on August 11, 2021. This report focuses on loadable data and software, primarily Aircraft Controlled Software (ACS). The software is controlled at an aircraft level, meaning it is treated as an aircraft part - Aircraft Controlled Loadable Software Part (ACLSP).

3.3 SAE AIR 7368

With the expectation for the FAA to update Parts 33 & 35 (engines and propellers) with 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.

Initial Ballot Closed December 9, 2021. Final ballot is expected in 2022.

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 2022).

4.1 ALPA / AIA Joint Recommendations

Over the last year the AIA Cybersecurity committee has engaged with the representatives of the ALPA organization in response to a paper which they published last year raising concerns about aircraft operational cybersecurity and the role of the pilot. The paper, and subsequent meetings which have been conducted between the groups, highlighted a gap in understanding between the pilot community and manufacturers in how cybersecurity is handled in design, certification, and operation of the aircraft. The approach today which is built on the work of RTCA and EUROCAE over the last 15 years follows the DO-326A/ED-202A standard. The standard outlines a risk-based approach like (and connected with) the safety design process meaning cybersecurity risks which could impact safety must be identified in the design process and mitigated to an acceptable level. Like safety this process includes evaluation throughout the complete development lifecycle of the aircraft system with objectives and activities incorporated into design, implementation, and verification; including, if necessary, any notification or relevant procedures prescribed for the pilot. This paper will explain in more common terms the process as it exists today, the gaps which have been identified as part of the meetings occurring during 2021, and recommendations for consideration in future design and testing. The goal is to ensure a correct balance can be struck between providing pilots actionable alerts and general situational awareness which could be helpful in completion of an aircraft's mission.

This paper projected to be published Q1 of 2022.

4.2 Software Security

Software, including executable code and databases, is critical for the safe operation of the complex electronics guiding and operating civil aircraft. As complex electronics are now ubiquitous on aircraft and increasingly no longer have mechanical backup, tampered software poses risks ranging from aviation safety to global aviation impact. This paper focuses on providing recommendations for securing software distribution and software loading (onto aircraft LRUs).

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.

With the release of security standard ARINC 645-1, updates to ARINC-667 pertaining to secure software distribution and configuration management, increasing availability of corresponding software security tools, and maturation of methodologies currently in use, guidance for compliance is necessary for the aviation industry. This paper seeks to address this and provides recommendations to standardize best practices as much as possible.

A 2021 version of the paper has been published in 2021. In 2022, the working group will continue by agreeing among aviation stakeholders the phased approach presented in the 2021 paper and this update is expected by the end of Q2 2021.

4.3 AIA Position on Cybersecurity Testing

Airplane manufacturers, airline/cargo operators, component suppliers, regulators, and those building and operating the infrastructure of the global aviation industry all have a common goal – SAFETY. As cybersecurity risk in the aviation industry continues to expand and evolve. Many aviation industry businesses and organizations are seeking methods to provide continuous assurance and validation, that the digital components of aircraft and supporting aviation infrastructure remain safe and uncompromised. AIA recognizes the evolving risks to digital components, the safety objectives of all industry stakeholders and the risks that may occur in testing previously certified airplanes and ground support equipment. Additionally, new cybersecurity risks may emerge after type certification that must be continuously reviewed and verified in terms of potential airplane and ground system impacts. AIA is also aware a growing number of operators have begun to pursue options to conduct their own technical risk assessments and testing or develop other means to understand risks that may emerge post type certification, either as newly identified vulnerabilities or through modifications or other configuration changes requiring Supplement Type Certification or other re-validation of the safety and security of the airplane and its components. AIA concurs with FAA, GAO, and industry standards stating concerns that cybersecurity testing of operational aircraft may have potentially severe consequences resulting in regulatory non-compliance and potentially creating a safety event. As such, AIA considers direct testing of operational aircraft should remain the very last alternative method to address cybersecurity risks. This includes reducing the potential for cybersecurity testing and other technical evaluation to negatively impact the integrity and safety of our civil aviation industry, including its airplanes and ground support services. Instead, AIA recommends aircraft manufacturers, component suppliers, and airline operators partner together on the development of methods and procedures are conducted in protected laboratory or other controlled environments with measures in place to ensure these activities cause no operational reliability concerns or additional safety risks to global air travel.

Full Whitepaper

4.4 Change Impact Analysis for Major/Minor Determinations

EASA's product security rules have entered into force in January 2021 anchoring cybersecurity in type certification of parts and products via AMC 20-42. As part of the amendments made by EASA, the guidance material for assessing changes to type certifications in 21.A.91 was updated to include a discussion that cybersecurity may lead to changes being classified as major. The FAA is preparing to release product security rules and as with EASA, cybersecurity will need to factor in assessing changes to issued type certification.

Upon review of the issued guidance material by EASA and the industry guidance in DO326A/ED202A and DO356A/ED203A, it was considered that available material does not provide instructions to ensure consistent approaches among applicants, clarity in (re-)verification activities needed and that the industry guidance is inconsistent with change impact processes from other related technical domains such as system, software and hardware engineering. As a consequence, AIA is analyzing available material from different technical domains to propose an appropriate change impact assessment for cybersecurity. The recommendation paper will make proposals on the necessary activities to analyze the impact of changes on cybersecurity and the verification activities necessary for the change.

This paper is projected to be publish in Q4 of 2022.

4.5 Supply Chain

The supply chain has not comprehensively been secured due to its excessive complexity. A single solution cannot address all the topics, nor offer the ability to harmonize and address the breadth and depth of the system. To make progress on the issue this report has developed a matrix to split the supply chain problem into more manageable sub-problems by 1) considering supply chain organizations as specific to aviation versus those that do not follow aviation regulations and practices, and 2) defining whether the supply chain delivers physical goods or soft goods (such as software or databases). Based on these sub-problems, a number of recommendations have been developed as specific solutions. The most important of these is the need for an aviation Information Security Management System (ISMS) properly tailored for the size, complexity and risk an organization faces. The report also provides next steps for implementing the recommendations including suggested standards and standards groups for producing published guidance. The recommendations of this report have been provided to the European Cyber security for aviation Standards Coordination Group (ECSCG) for consideration.

A completed draft of this paper is currently in review by the AIA Cybersecurity Subcommittee and an interim version is expected to be published by the end of Q1 2022. Work will continue throughout 2022 on expanding guidance on supply chain security.

Appendix A: Members & Contributors

AIA Working Group Members

Mayank Agarwal	Infosys	Tom McGoogan	Boeing
Ruchik Amin	GE Aviation	Moraes, Polina	Embraer
David Almeida	LS Technologies	Patrick Morrissey	Collins Aerospace
Tim Anstey	Boeing	Tim Murnin	Amazon
Steve Benham	GE Aviation	Siobvan Nyikos	Boeing
Majed Bouzouita	Boeing	Gerry Ourada	Lockheed Martin
John Bush	Boeing	Suzanne Patterson	Boeing
Brian Connolly	Boeing	Scott Pepper	Boeing
Michael Cook	ATI Metals	Caroline Prado	Boeing
David De Meulder	Aerion Supersonic	Greg Rice	Collins Aerospace
Kathleen Finke	Astronautics Corp. of America	Leslie Riegle	AIA
Michael B Fox	L3 Harris	James Robinson	Boeing
Matt Gomez	Bell	Aloke Roy	Honeywell
Todd Gould	Boeing	Stefan Schwindt	GE Aviation
Tim Harris	ATI Metals	Jason Shuler	Astronautics Corp. of America
Aaron Hurst	HEICO Aerospace	Sam Singer	Boeing
Nicole Jolly	Booze Allen Hamilton	Sean Sullivan	Boeing
Corey Jones	Boeing	Ryan Terry	Lockheed Martin
Dave Jones	Astronautics Corp. of America	Nora Tgavalekos	Raytheon
Bret G Lynch	Pratt & Whitney	Jason Timm	AIA
Laurel Matthew	Boeing	Jeff Troy	GE Aviation / A-ISAC

Steven Marchegiano	ADI American Distributors

Cyber Working Group Guests/Observers:

Daniel Diessner	Embry Riddle	Kanwal Reen	Collins Aerospace
Gabe Elkin	MIT Lincoln Lab	Ted Rush	FAA
Will Gonzalez	FAA	Rob Segers	FAA
Sidd Gejji	FAA	Remzi Seker	Embry Riddle Aeronautical University
Jerry Hancock	Inmarsat / ASD	Randy Talley	ACI Tri-Chair DHS CISA
Ayan Islam	DHS CISA	Julien Touzeau	Airbus
Theodore Kalthoff	Bombardier	Lt Col ERIC D. TRIAS	USAF
Terry Kirk	Aviation ISAC	Isidore Venetos	FAA
Varun Khanna	FAA	Keith Wallace	FAA
Jennifer Miosi	United Airlines	Philip Windust	FAA
Samantha Lopresti	FAA	Hank Wynsma	United Airlines
Steve Ramdeen	FAA		