Cybersecurity Industry Assessment & Recommendations

Report to the AIA Civil Aviation Council
September 2020

Civil Aviation Cybersecurity Subcommittee

Dan Diessner – Chair (The Boeing Company)
Hank Wynsma – Vice Chair (GE Aviation)
Leslie Riegle – AIA Leader
Patrick Morrissey – Editor (Collins Aerospace)

Contents

1 INTRODUCTION

Cybersecurity continues to gain importance within the aviation industry, driven by its relationship to safety as well as technological and societal forces. Aircraft, airports, and other elements of the air transport system are increasingly connected, supporting both a greater number of physical connections (wired and wireless) as well as a greater variety of protocols and services carried over those connections. This digitalization brings operational and maintenance efficiencies but also greatly increases the complexity of aviation systems and their exposure to cyber threats.

Industry is continuing to grow on the momentum established 5 years ago. Standards committees are continuing to work together to harmonize standards between the E.U. and the U.S. Participation in industry coordination (e.g. ICCAIA, AIA, ASD, and IATA) by OEMs, suppliers, and airlines remains strong as designers and operators work together to advocate for changes and collaborate on solutions.

Interest in the cybersecurity posture of aviation systems is growing within the security research community. The DEF CON security conference hosted its first Aviation Village in 2019 and hosted a revamped and expanded virtual Aerospace Village for 2020. Published conference talks on operational aviation systems and an aerospace capture-the-flag exercise received considerable media coverage.

Internationally, ICAO published its Aviation Cybersecurity Strategy in October 2019, and work by the Secretariat Study Group and Data Communications Infrastructure Working group continues. Additionally, in early 2020, ICAO launched the Trusted Framework Study Group to define the foundations for securing tomorrow's aviation communication through network separation and data assurance. AIA, thru the work of the AIA Civil Aviation Cybersecurity Subcommittee, diligently continues to drive the U.S. OEM perspective and provide inputs to these forums via the ICCAIA Security Committee.

In the U.S., the FAA, AIA, and standards bodies recognize the growing attack surface and are focusing the advancement of regulations and standards to support the industry. The U.S. also updated its National Strategy for Aviation Security in December 2018 and created an Aviation Cyber Initiative (ACI) with representation from the departments of Homeland Security, Defense, and Transportation to coordinate risks, capabilities, and solutions across the various departments. The AIA Civil Aviation Cybersecurity Subcommittee has led the charge, in cooperation with the FAA, to organize and define the Cyber Safety Commercial Aviation Team, and is coordinating with CAST for a cooperative and potentially conjoined path forward.

In Europe, EASA published amendments to the Commercial Specifications to guide cyber considerations throughout the product lifecycle. The European Strategic Coordination Platform (ESCP) for Aviation Cybersecurity published its Strategy for Cybersecurity in Aviation and is working on a horizontal cybersecurity rule which will include Information Security Management Systems (ISMS) in aviation organizations. The Civil Aviation CyberSecurity Task Force (CACS-TF) within the Aerospace and Defence Industries Association of Europe (ASD) is also supporting a variety of EASA tasks such as management of information security risks and production of acceptable means of compliance for newly issued E.U. rules for all certified parts. The AIA Cybersecurity Subcommittee continues to partner closely with its peer organization in Europe, ASD, to pursue harmonized U.S. / E.U. positions.

2 Reflections on COVID-19 and the Industry

The COVID-19 pandemic has had a significant impact on the aviation industry due to the travel restrictions and resulting decrease in demand for airplanes. Even as travel restrictions lift, the flying public may be slow to travel again at the frequency seen in previous years. The pandemic has changed our way of life and how we

do business. From aviation cyber industry standards committee meetings to popular security conferences, events are either cancelled or moved to a virtual format. To address the economic downturn, and associated reduction in travel, organizations that serve the aerospace industry have had to employ furloughs, early retirement programs, and in some cases even layoffs, which will result in a loss of expertise. Airlines are retiring aircraft early which can result in more equipment available to the research market. Aircraft moved into storage will need to be evaluated for compliance before returning to service. In addition, to these effects, there are members of the aviation cybersecurity community who have personally been impacted by COVID-19 and are either recovering from it or supporting family members as they recover. But in the face of adversity we also recognize our mission is longer term. Technology and how it's implemented in the aerospace system continues to evolve and the work we do within the industry today lays the foundation for tomorrow. So while we cannot meet in person, we continue our work and collaboration across the industry virtually, advancing cybersecurity within aerospace, and advocating for common standards and regulation which support a proper balance of requirements and design decisions enabling industry participants to flourish tomorrow beyond today's challenges.

3 ASD Activities

Aerospace and Defence Industries Association of Europe (ASD) is the voice of European Aeronautics, Space, Defence and Security Industries, representing over 3,000 companies and actively supporting the competitive development of the sector in Europe and worldwide. It has direct members, active in 18 countries, including 18 major European industries and 23 National Associations. Together, ASD members employ more than 870,000 people and generate a turnover of over €246 billion. Within its Civil Aviation Business Unit, the Civil Aviation CyberSecurity Task Force (CACS-TF) comprises of cyber experts from companies serving both ANSPs and Aircraft manufacturing and is responsible for cybersecurity matters.

ASD is a member of the European Strategic Coordination Platform for Cybersecurity in Aviation (ESCP), which is a co-operative partnership created to define and coordinate the implementation of a European Strategy for Cybersecurity in Aviation. The CACS-TF is currently supporting and orienting the European Union Aviation Safety Agency (EASA) in the definition of RMT.0720 Management of Information Security Risks. This RMT envisages the creation of a dedicated E.U. Regulation by 2022 designed to efficiently contribute to the protection of the aviation system from cybersecurity (information security) attacks and their consequences through an information security management system.

The CACS-TF has also been active in RMT.0648 Aircraft Cybersecurity through the ESCP. The specific objective of this task is to mitigate the safety effects stemming from cybersecurity risks due to acts of unlawful interference with the aircraft on-board electronic networks and systems. This resulted in the Certification Specifications on CS-25, CS-29, CS-27, CS-23, CS-E, CS-ETSO and CS-P, (for detail see Section 4.2).

The CACS-TF is also providing significant support to EASA, through the ESCP, in the production of Guidance Materials (GM) and Acceptable Means of Compliance (AMC) that are needed for the implementation of the E.U. rules (i.e. RMT.0720 and RMT.0684). This is linked to the work carried out in STORM and the European Cyber Security for Aviation Standards Coordination Group (ECSCG), whereby ASD has been a main contributor to the ECSCG's rolling development plan.

The CACS-TF is also working with the ASD Airworthiness Committee to identify potential convergence between compliance and implementation of Safety Management System (SMS) (https://www.asd-europe.org/sites/default/files/atoms/files/SMS%20Standard_final%20issue%20A_20180917.pdf) and

compliance to RMT.0720 with the same objective of proposing guidelines to the different stakeholders by end of 2021.

The CACS-TF is also active in coordinating and cooperating with other stakeholders. For example, within the manufacturing sphere, this involves working with other ASD groups (e.g. UAS, UAM, ATM) and AIA and the International Coordinating Council of Aerospace Industries Associations (ICCAIA). Cooperation and coordination also extends further to other stakeholders (e.g. A4E, ACI, CANSO, and IATA). The CACS-TF has prepared a questionnaire to find out airlines' perception of cybersecurity, which was pushed to ICCAIA in Q1 2020 for review and is now available under A-ISAC umbrella. A key motivation behind this is to build trust between the manufacturers and the end users (airlines). The Aviation ISAC-Europe, A4E and IATA have circulated the questionnaire to its airline members and results are expected end of 2020.

4 Regulatory Progress

4.1 U.S.

The FAA is in the process of proposing rulemaking for Part 25 category aircraft. The DRAFT NPRM is going through internal coordination, resolving comments received within the FAA. Afterwards, it is expected to be published sometime in the summer of 2021 for comment by the public. After receiving and resolving comments, the rule will be published during the first of the year 2023. In the meantime, the FAA is updating several Issue Papers to reflect current Aircraft Systems Information Security Protections (ASISP) trends and is expected to publish those prior to rule completion/publication. Along with the proposed rule, the FAA is drafting Means Of Compliance (MOC) Issue Papers (IP) that include the Special Conditions (SC) and point to industry standards for the Accepted MOC. This approach is quicker than drafting an Advisory Circular (AC) indicating that applicants can use DO-326A and DO-356A. Regulatory action for Parts 27, 29, 33 & 35 are in exploratory stages. For those parts, the FAA is evaluating the risks based on past and current FAA certification projects in those parts involving Issue Papers on cybersecurity risk and will determine if their current rules are adequate for cybersecurity protection. For Part 23, the FAA is actively engaged with ASTM F44 committee and supports the work on this best practice standard through small airplane standards staff who are involved in F44. For more information on this standard within F44 see Section 7.1.3.

4.2 E.U.

The European Union Aviation Safety Agency (EASA) has concluded their Rulemaking Task RMT0648 introducing cybersecurity rules for products, parts and equipment which will become applicable in January 2021. The rules are for all certified parts:

- CS-23 (Small Airplanes)
- CS-25 (Large Airplanes)
- CS-27 (Small Rotorcraft)
- CS-29 (Large Rotorcraft)
- CS-E (Engines)
- CS-P (Propellers)
- CS-ETSO (European Technical Standard Orders)

CS-ETSO has had cybersecurity added to the general section applicable to all ETSOs. All Certification Specifications use a common Acceptable Means of Compliance AMC 20-42 referencing ED202A/DO326A,

ED203A/DO356A and ED204/DO355. In addition, Part 21 was amended for clarifying cybersecurity aspects in major change determination. AIA has submitted comments on NPA2019-01 announcing the proposed rules of RMT0648, most of which have been accepted and adopted by EASA. The comments received and their response can be seen in CRD 2019-01. (See EASA website: https://www.easa.europa.eu/document-library/agency-decisions/ed-decision-2020006r)

EASA is in the process of proposing rules for information security management systems for all approved aviation organizations. In Europe, more organizations require an approval than under FAA jurisdiction – for AIA members the most notable approvals are Design Organization Approval (DOA – Part 21 Subpart J), Production Organization Approval (POA – Part Subpart G) and Maintenance Repair Overhaul Organization Approval (CAMO/CAO/Part 145). NPA 2019-07 has been issued detailing a proposed Part AISS that would introduce rules for all approved organizations to implement and demonstrate an Information Security Management Systems that – analogous to existing Safety Management System requirements – would require the approved organization to identify threats to safety related information assets and secure them appropriately. These rules would also apply to the supply chain of the approved organization – whether for suppliers of hardware and software for integration into a part as well as suppliers or service providers of relevant IT assets. EASA has already gathered comments from public consultation of NPA 2019-07 and is aiming to release an Opinion to the European Commission proposing a rule. The European Commission typically takes one year to assess the rule and release it through the comitology process with the E.U. Member States. To aid the rulemaking process, EASA has established the European Strategic Coordination Platform (ESCP) to consult with stakeholder groups (E.U. Commission, E.U. agencies, E.U. member states, and industry organizations representing the different stakeholders in aviation) on the rules. AIA has observer status within the ESCP and has contributed comments to NPA 2019-07. EASA is planning to issue the opinion in March of 2021 and the ESCP is now focusing attention on discussing and establishing the Acceptable Means of Compliance and Guidance Material for the new rule.

5 Industry Collaboration

5.1 Aviation – Information Sharing and Analysis Center (A-ISAC)

The Aviation Information Sharing and Analysis Center is a member-driven, non-profit cyber security information sharing community for the global aviation eco-system. Members include OEM's, supply chain, airlines, airports, aviation communications, air navigation service provider and other companies serving the aviation industry. The A-ISAC works across the industry with its members to facilitate communication and coordination of threats in the ever changing adversary landscape. Below is a list of ongoing endeavors and specific thrusts by the organization and its members:

- Third Annual Aviation Cybersecurity Survey published in February 2020: The Aviation ISAC created and published its third annual Aviation CISO survey. The survey creates a risk register for the industry as it highlights the cyber security areas of focus for the global Aviation Industry. The Aviation ISAC held 3 series of Roundtables in Feb, April and July to address previously identified and emerging cyber risk. This year was particularly significant in light of risks identified due to a major industry slowdown and the workforce moving to remote locations.
- Security research and vulnerability reporting: The Aviation ISAC is a coordination hub, linking aviation cybersecurity researchers with the owners and developers of applications, systems and products which may be vulnerable to attack. Just this year the Aviation ISAC connected 8 researchers with both member and non-member companies on vulnerability claims impacting the industry. The Aviation

ISAC funded the delivery of the DEFCON Aerospace Village Cyber Challenge to continue to build relationships with emerging researchers in the industry.

- Global Partnership Building. The Aviation ISAC continues to build global partnerships on threat intelligence, best practice sharing, along with standards and policy development with Aviation stakeholder associations. These relationships have led to the delivery of actionable intelligence which has enabled companies to reduce risk on their networks and products. We are actively contributing to work being done with AIA, ICAO, EASA, EuroControl, ESCP, AIAA, UK NCSC, and numerous other agencies.
- Ransomware Initiative: The Aviation ISAC has taken the lead as a part of the National Council of ISACs to address the dramatic increase in ransomware. Similar to ransomware attacks on airports and airlines, critical infrastructure across the U.S. is being significantly impacted. As a result, the Aviation ISAC led a team which authored a whitepaper on the issue, released in August 2020. The whitepaper highlights the alarming growth in the number of ransomware events and their destructive impact on businesses. The paper calls for better regulation and an acceleration of investigations.
- Global Airline Cybersecurity Survey: The ICCAIA has drafted a survey of airlines to explore the cross-function coordination between Chief Safety Engineers and Chief Information Security Officers. The Aviation ISAC is funding the survey and acting as the agent to distribute, collect and analyze the results. The survey results will be presented at the Aviation ISAC Summit in September 2020.
- Aviation Supply Chain Security: The Aviation ISAC has opened up its Daily Aviation and Weekly Aviation Threat Intelligence Products to the entire industry for free through the end of 2020. In addition, for member companies, we have secured free scanning of external facing network connections of their suppliers. This limited offer is greatly increasing the security conversations across the industry.
- The Aviation ISAC will hold its 7th Summit virtually on Sept 23-24th.

5.2 Aviation Cyber Initiative (ACI)

On May 30, 2019 the Secretaries of the Department of Defense, Homeland Security, and Transportation ratified the Aviation Cyber Initiative (ACI) charter establishing the ACI Tri-Chair task force. ACI focuses on supporting the National Strategy for Aviation Security's (NSAS) cyber objectives by identifying shared aviation cybersecurity risk and pursuing priorities that support resiliency in the aviation ecosystem. The ACI Tri-Chair Executive Committee (EXCOM) coordinates and aligns Department interests, authorities, policies, and missions in support of the NSAS through its priority initiatives:

- ACI Communication Plan: The primary goal of the ACI communication plan, and ACI Charted-directed plan, is to support the mission of the ACI by providing a consistent approach to messaging and engagements within ACI's scope of responsibilities. The ACI communication plan ensures interagency unity of messaging on aviation cybersecurity initiatives, establishes a consolidated communication methodology internally within its respective core organizations and establishes guidelines for providing timely dissemination information to its stakeholders.
- Joint Interagency - Ground Air Transponder Operational Risk Reduction (JI-GATOR) Initiative: This effort developed and tested non-material aviation transponder Tactics, Techniques and Procedures (TTP) to mitigate Aviation transponder Operations Security (OPSEC) and Automatic Dependent Surveillance-Broadcast (ADS-B) spoofing vulnerabilities. JI-GATOR completed flight testing with units from the Air Mobility Command, Customs and Border Protection, and the U.S. Coast Guard; completed ADS-B spoofing mitigation testing at the FAA William J. Hughes Technical Center; and

completed a study of the FAA's Sensitive Data Program. JI-GATOR efforts produced TTP to reduce aviation transponder data confidentiality, integrity and availability vulnerabilities with a final report due October 2020.

- ACI Legal and Policy Gap Analysis Tabletop Exercise (TTX): On June 30, 2020, the ACI completed a National Security Council tasked exercise with participation from DHS, FAA, DoD, A-ISAC, and industry partners. The coordinated final report, due in October 2020, includes key observations and recommendations to remediate cybersecurity legal and policy gaps between commercial civilian and military aviation within the Aviation Ecosystem.
- Aviation Cyber Workforce Development: ACI is developing cybersecurity and resilience curriculum for aviation ecosystem personnel. ACI participated in six DHS-led Airport Cybersecurity Training courses in CY19 and CY20. ACI member Departments, Idaho National Laboratory, and Embry-Riddle Aeronautical University are collaborating on an aviation focused training program from existing course offerings.
- National Federation of Aviation Cyber Test Organizations and Resources (N-FACTOR): ACI established the N-FACTOR on June 3, 2020 to accelerate aviation cybersecurity risk-reduction and resilience initiatives. The FAA Tech Center, Johns Hopkins Applied Physics Laboratory, and MITRE are leading the effort to develop a research-oriented, accessible, and searchable National Aviation Cyber Resource Guide. In addition to government laboratories, initial participants include Federally Funded Research and Development Centers, University Affiliated Research Centers, National Labs, and industry partners. Additionally, in July 2020, nearly 100 subject matter experts convened to collaborate and coordinate resource requirements and contribute expertise across ten aviation cyber initiatives.
- Aviation Cyber Remote Attestation Integration and Demonstration (RAID) Sub-Working Group: ACI established the RAID Sub-Working Group to increase public, private, and academic knowledge and confidence in cyber attestation technology. Cyber Attestation fills a critical gap in the ability to detect and identify cyber anomalies and support approved-baseline restoration. The inaugural RAID Sub-Working Group included 45 participants from DOD, DHS, FAA and industry. The Air Force Research Laboratory (AFRL) plans to demonstrate attestation technology on a commercial-derivative aircraft (KC-46) for the RAID Sub-Working Group in Q3/Q4 CY2020 or as COVID-19 conditions permit. Results from this demonstration will support further collaboration efforts to develop deployable cyber attestation technology for the civilian and military aviation sectors.
- Small Business Innovation Research Project V-Fortified Instrumented Bus Reliability Activity Net Tracker (VIBRANT): ACI is co-sponsoring a Small Business Innovation Research (SBIR) program to develop technologies that detect real-time anomalies and intrusions on aviation data buses. The VIBRANT project supports an Artificial Intelligence/Machine Learning (AI/ML) enabled aviation data anomaly and intrusion detection capability to support System Integration Laboratory (SIL) testing and to be used on operational avionics 1553/429 data bus.

5.3 IATA

Over the course of the last year, it has become apparent through interactions in a variety of forums, that there is a fundamental disconnect between the OEM and airline views and concerns around cybersecurity. Not surprisingly, the organizations come at the problem from two different perspectives.

OEMs and suppliers develop highly complex embedded systems based on strict guidelines and requirements to ensure the safe operation of the aircraft. Aspects of cybersecurity are integrated into the systems design

process at each stage of aircraft development. Not surprisingly, a cross section of these companies and their engineers have been engaged in the development of standards over the past decade. Developing DO-326A/ED202A, DO-356A/ED203A, DO-355A/ED204A, all of which will guide current and future design for the connected aircraft. But the technical details of how the aircraft is protected through the airworthiness instructions provided to the airlines have not been easy to understand and incorporate.

As operators, the airlines have minimal involvement in the design process but are critical consumers and practitioners of the instructions for continued airworthiness (ICA). For them, the aircraft is a purchased device which will be attached to their company network and needs to be maintained not only for security but for safety. Historically, continued airworthiness issues are managed in service organizations which have established processes for handling quality issues, reporting problems, and resolving them in concert with the regulators, OEMs and suppliers. Personnel in these organization do not have the foundations for cybersecurity. Conversely cybersecurity experts within the airlines, commonly found in IT support organizations, do not have the foundational knowledge of aircraft systems and operational maintenance procedures to manage it out of the gate. The result is steep learning curves for each organization to take on in addition to building bridges between organizations.

In recent months, working through ICCAIA; AIA, ASD, and IATA have established a working group to facilitate better communication between the operators and suppliers. The group aims to provide more visibility into the design and development processes for operators and better understanding of the problems and concerns of managing operations for the suppliers. Such collaboration is critical to the shared risk presented by cybersecurity. The group plans to use industry forums to organize workshops and help narrow the divide through knowledge sharing, establishment of a common needs definition and continued collaboration to harmonize process and information exchange to meet the greater needs of the industry.

Finally, in light of the pandemic and high volume of parked aircraft, AIA working in conjunction with ASD & IATA through ICCAIA, has put forth recommendations for cyber security considerations as part of return to service guidance for parked aircraft. The guidance includes considerations for ensuring the integrity of the aircraft and its systems were maintained during storage in a proper configuration and ensuring as they rejoin the airspace and associated networks that they are up to date with the latest versions of software and databases as appropriate for the systems. The guidance was developed by the OEM and supplier community and flowed to ICAO to flow to the owner operator community

5.4 ICAO Data Communication Infrastructure Working Group

The ICAO Aeronautical Communication Panel (ACP) – Data Communication Infrastructure Working Group (DCIWG) was formed to work technical aspects under the ICAO Air Navigation Commission. CP-DCIWG been tasked to develop Standards and Recommended Practices (SARPs), as well as, guidance material for air-ground and ground-ground aeronautical communications for both data and voice as they transition to an Internet Protocol Suite. This work is being performed under two different tasks with each responsible for several technical manuals.

The first, Job Card CP-DCIWG.006.02 – Provisions on the exchange of information using the aeronautical telecommunication network over the Internet Protocol Suite. An IP-based network for ATM is a key enabler for developments such as SWIM, FF/ICE, TBO and RPASs and many others. However there are complex issues that need to be addressed to ensure network security and mobility across various media. Under this tasking the group is updating:

- DOC 9896 – Manual for the ATN using IPS Standards and Protocols, Version 3. Updates will be made to account for required security, mobility, performance, addressing and naming conventions in the management of ATN Systems, and

- Annex 10 – Vol III, to amend with updates on addressing and naming conventions, their management and security.

The second, Job Card DCIWG.007.02 - SARPS and Guidance on the Cyber-Security of Air Navigation Communications. 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 ATM system. SARPS and guidance will be needed across a whole range of areas, especially those related to Information Management (IM) and Communications. In addition to this, the automated systems used to support operational improvements such as FF/ICE, CDM, TBO and RPAs will require protection against external intrusion. Under this tasking the group is updating:

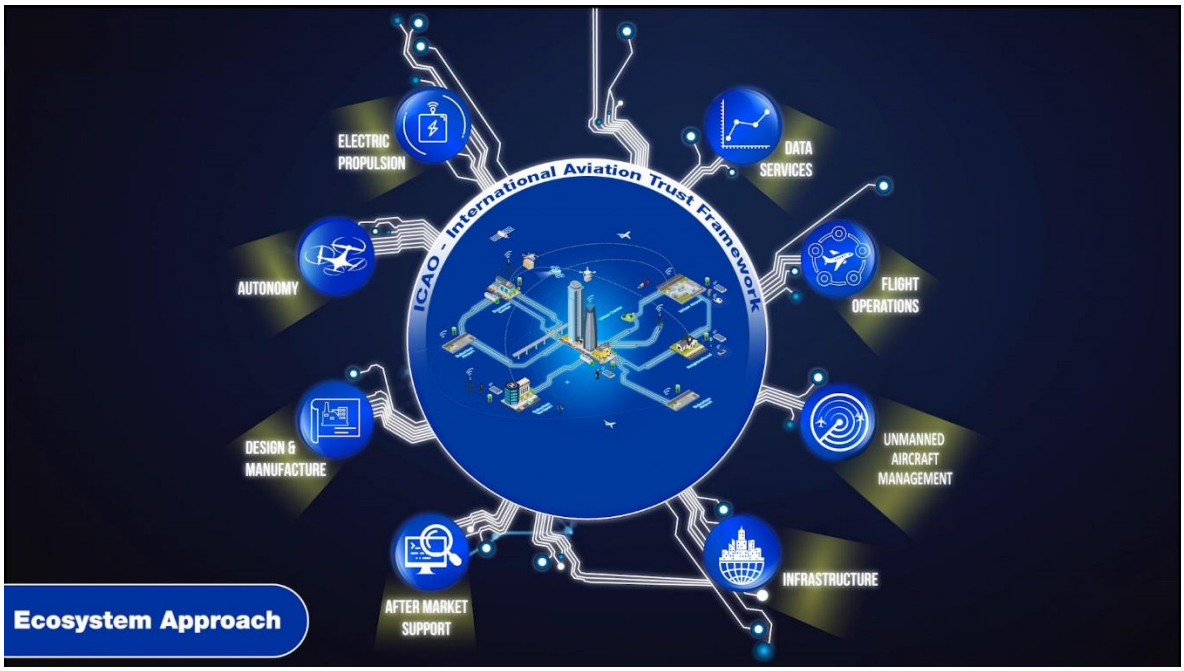
- Annex 10 Vol II/III with amendments related to air navigation security, and
- Doc 9985 – ATM Security Manual, with amendments related to air navigation security

To provide a more dedicated focus on the technical aspects of moving to IPS for ATM, Working Group I was established under the CP-DCIWG. WG I is concentrating on the completion of several detailed technical specifications for ATN and will complement the SARPS for ATN/IPS. WG I is broken into two main activities, The IPS Mobility Subgroup and the IPS Security Subgroup. The Mobility subgroup is working to solve aviation unique challenges associated with the speed at which aircraft fly and their connectivity to different ground networks as an airplane crosses different Communication Service Provider (CSP) coverage areas. The IPS Security subgroup, on the other hand, is focused on ensuring that cybersecurity threats that could negatively affect air traffic safety services are accounted for in the design and architecture of both the air and ground assets that will make use of IPS. Deliverables for WG I include:

- DOC 10090 - Manual of Security Services for Aeronautical Communications
- DOC 10095 - Manual of Public Key Infrastructure (PKI) Policy for Aeronautical Communications
- DOC 10145 - Manual of Security Risk Assessment for Aeronautical Communications

5.5 ICAO Trusted Framework Study Group

As the global aviation ecosystem transforms from a carbon based world to a digital based world, the evolution of systems for identity management, data/information processing and digital communications pose new concerns regarding the effectiveness of existing security architectures, procedures and processes in the global aviation community. This digital transformation cuts across the aviation ecosystem. ICAO is leading the evolution to a digital “Global Aviation Trust Framework” that will help integrate a harmonized and secure approach for aviation interoperability in a digital world. Cyber events are becoming recognized by the global aviation community as potential risks to authentication, access to critical aviation infrastructure, safety of aircraft, and the safe operations of the airspace. These risks include disrupting air navigation and other related services that could have both efficiency and safety implications.



In 2018, ICAO established, under the Air Navigation Bureau, the Trust Framework Study Group (TFSG) in order to develop a common set of principles, policy, guidance, and a transition strategy for a globally harmonized trust framework, that will enable trusted ground-ground, air-ground and air-air exchange of data and information among aviation and non-aviation stakeholders taking into account relevant technologies, including the Internet. This trust framework should consider and incorporate future industry needs for both existing airspace users and new entrants and provide the level of resilience and interoperability needed for the continued safe operations of the civil aviation system.

The work of the study group is divided amongst three working groups: Digital Identity (DI), Globally Resilient Aviation Interoperable Network (GRAIN), and Trust Reciprocity Operational Needs (TRON).

The Digital Identity working group is focused on defining an interoperable infrastructure to support integrity, authenticity, and non-repudiation of data exchange in the aviation ecosystem. The group is developing a certificate policy (CP) and guidance materials which could provide a foundation for a centralized or distributed (via federated trust) PKI infrastructure. Once in place and operational, the infrastructure would provide the ability to replace paper processes with electronic, such as aircraft registration, licensing, and transfer, or maintenance operations. It could also provide the basis for trusted software delivery and loading, or authenticated communications between the aircraft, airlines operations, and ANSPs.

The GRAIN working group is defining a set of minimum requirements to ensure authentication, integrity, confidentiality, levels of service (availability, performance), authorization and resilience (to internal and external threats) and to allow information exchanges among the 6A's (aircraft, airports, airlines, airlift, aviation management and actors) using a global architecture of federated interconnected networks. Within a common trust model, the minimum requirements should be transport agnostic to allow stakeholders to select the appropriate technologies for information exchange based on individual risk and performance needs. The resulting network would provide the community with a common trust foundation through which trusted communications could be driven. This common set of requirements will help provide a comparatively higher

quality of service (availability) and integrity through their application and compliance, similar to what's done for international finance today but with different requirements.

The TRON working group is evaluating and developing use cases for the GRAIN and DI working groups by looking. Looking at the many operational and maintenance use cases of the Aerospace industry. Through their work they decompose human, electronic, and paper processes which support the industry and consider the security gaps within those processes. In doing so they are exposing areas of risk which could be addressed through the technologies envisioned by the DI and GRAIN working groups, driving discussion, and building consensus around which use cases are the correct scope to pursue and which ones are best left to industry participants to solve individually due to constraints of cost, complexity, or politics.

6 Unpiloted Aircraft System Considerations

The introduction of Unpiloted Aircraft Systems (UAS) into the airspace system offers unique complexities and risks to the system which must be managed to support the continued safety for all participants. In the UAS space, there is a size/weight category which separates hobby operations from commercial. Similarly, a further use of autonomy in business and air transport operations blurs the line between 'heavy UAS' operations and automated air transport operations. Autonomous operations of any commercial class operating in controlled airspace must have the capability to file, execute, modify, and close flight plans in order for the air traffic operators to manage vehicle separation in the global airspace. Additionally, all the aforementioned activities need to be executed with high integrity to ensure changes to the plan only occur pursuant to a defined process (i.e. no hacking the UAS via operational communications). All this requires increased integrity across the spectrum from assured processing, to vehicle registration, to authenticated communications, to non-repudiation in plan filing, execution, modification, and closure. In addition to integrity of Command and Control (C2) data links, industry also needs to address potential threat sources in the Detect And Avoid (DAA) supply chain, development, and operational environments.

As the community engages in discussions on these topics many different standards organizations and bodies are working through the varied use cases to provide new standards and guidance to the OEMs, operators, and maintainers to ensure autonomous systems are adequately equipped to support the needed cyber-resilience of the larger interoperable system.

6.1 Vehicle and Operator Certification

6.1.1 Design Regulation & Guidance

Currently within the U.S. the community is looking toward the standard being developed by the aforementioned ASTM F44.50 Working Group, "Standard Practice for Protection of Aircraft Systems and Information Security from Intentional Unauthorized Electronic Interactions". This standard which is intended to provide design guidance to Part 23 class 1-3 vehicles is being additionally considered as a baseline for a many classes of UAS vehicles due to similar size, weight, and operational use cases.

Having said that, regulations and guidance for how unpiloted and remotely piloted vehicles are certified will not be a one-size-fits all solution. In addition to size/weight considerations, there are differences in CONOPS between private, commercial, and defense. There are also varying levels of autonomy, e.g. remotely piloted one-to-one, remotely piloted one-to-many, and a truly autonomous air vehicles. These classifications must be carefully defined with the appropriate regulations and industry guidance assigned. While means of compliance and risk assessment methods can be borrowed from existing guidance, tailoring must be done as impact is defined differently and threats come from different sources.

Recommendation: Industry needs to rethink Design Assurance Levels (DAL) as traditionally low DAL systems (e.g. cameras) as low cost COTS components will have an increasingly important function in the mission and safety as levels of autonomy increase. Risk impact needs to be measured differently. If there are no crew or passengers, loss cannot be defined in terms of injury and loss of life as is used with DAL. However, there still need to be concern for the safety of people on the ground.

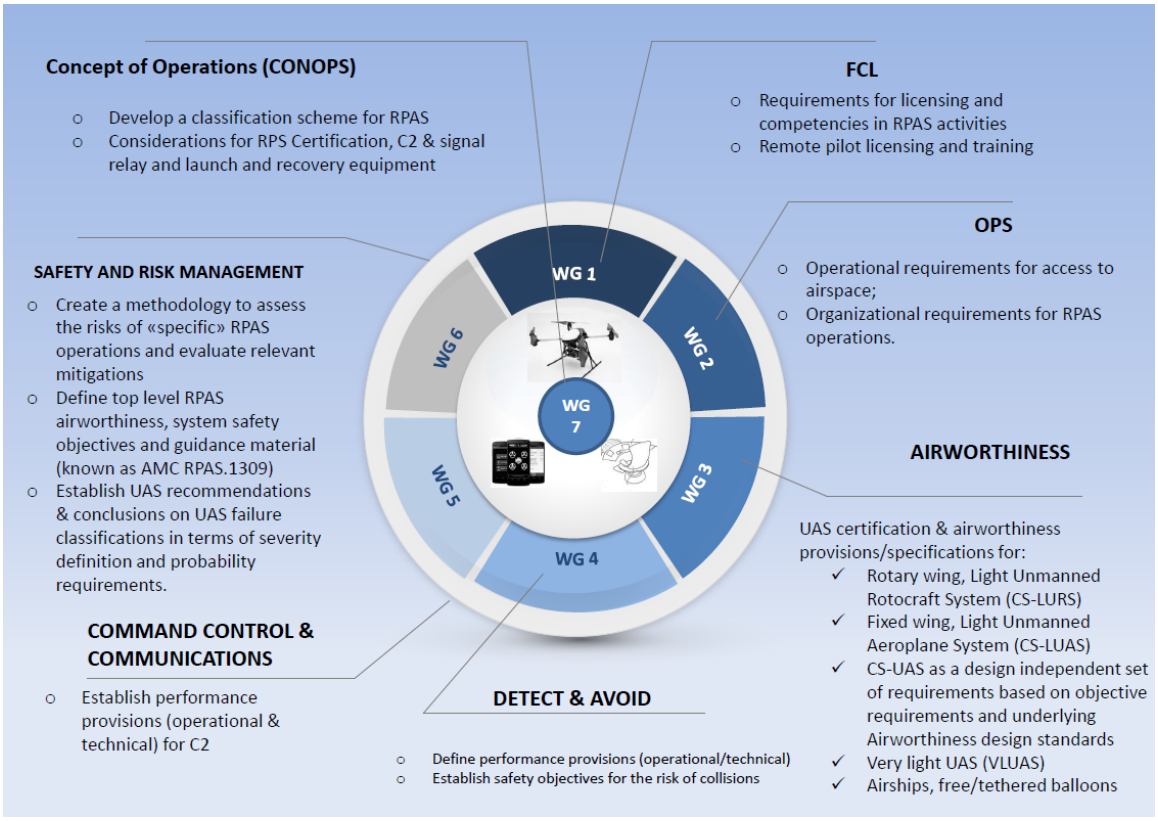
6.1.2 JARUS/WG-6

Joint Authorities for Rulemaking on Unmanned Systems (JARUS) is a group of experts from the National Aviation Authorities (NAAs) and regional aviation safety organizations which is using a holistic approach to addressing cyber security for UAVs. Its purpose is to recommend a single set of technical, safety, and operational requirements for the certification and safe integration of Unmanned Aircraft Systems (UAS), specifically including Remotely Piloted Aircraft Systems (RPAS) into airspace and at aerodromes. The objective of JARUS is to provide guidance material aiming to facilitate each authority to write their own requirements and to avoid duplicate efforts. If this harmonized guidance is endorsed by the authorities, this will facilitate the validation process of foreign certificates/approvals.

This requires review and consideration of existing regulations and other material applicable to piloted aircraft, the analysis of the specific risks linked to RPAS, and the drafting of material to cover the unique features of RPAS. UAS includes an aircraft and its associated elements which are operated with no pilot on board; this superset category can include both autonomous and remotely piloted vehicles. RPAS includes: a remotely piloted aircraft, its associated remote pilot station(s), the remote pilot(s), the required command and control links, and any other components required for the approved operation. RPAS is the initial priority for JARUS work, but broader needs for UAS may also be addressed.

At present, 61 countries' national authorities, as well as the European Aviation Safety Agency (EASA) and EUROCONTROL, are contributing to the development of JARUS. Since 2015, the Stakeholder Consultation Body (SCB) representing all industry communities of interest has also been established to provide support to all JARUS activities.

JARUS is broken up into different working groups as illustrated below.



Working Group 1 addresses Flight Crew Licensing, Working Group 2 addresses Operations, Working Group 3 addresses Airworthiness, Working Group 4 addresses Detect & Avoid, Working Group 5 addresses Command, Control, & Communications, Working Group 6 addresses Safety & Risk Management and Working Group 7 addresses Concept of Operations.

Working group 6's Specific Operator Risk Assessment (SORA) and Standard Scenarios document recommends a risk assessment methodology to establish a sufficient level of confidence that a specific operation can be conducted safely. Along with the document there is the Executive Summary and the Annexes: Annex A - Guidelines on Collecting and Presenting System and Operation Information for a Specific UAS Operation, Annex B - Integrity and Assurance Levels for the Mitigations used to Reduce the Intrinsic Ground Risk Classes, Annex C - Strategic Mitigation Collision Risk Assessment, Annex D - Tactical Mitigations Collision Risk Assessment, Annex E - Integrity and Assurance Levels for the Operational Safety Objectives (OSO) and Annex I - Glossary of Terms.

The current SORA process identifies safety risks, or threats, resulting from equipment failure, operator error, adverse operating conditions, etc. and then defines appropriate means for risk mitigation. The current SORA process, however, does not include a mean for assessing the safety risks introduced by a targeted or inadvertent cyber-attack. Since the October 2018 JARUS Plenary Meeting in San Diego, WG-6 (Cybersecurity) has developed the concept of an approach for the inclusion of cybersecurity considerations into the SORA as illustrated via examples in the cybersecurity annex of the SORA.

The AIA cybersecurity working group supports the work plan for WG-6 as the correct direction for the advancement of operational approval.

Recommendation: The FAA should: engage with JARUS WG6 on cybersecurity, evaluate the use of JARUS methods for MOCs, and work to support harmonizing methodologies with EASA and other CAA's for joint global endorsement.

6.1.3 Work at ICAO

There are two certified entities involved in traditional aircraft operation today: the vehicle, and the pilot or operator. Vehicles are registered so they can be identified and ownership managed across nation states. Operators need to be certified to demonstrate they have completed the required training and are knowledgeable enough to operate the vehicle safely in adherence to the rules and regulations for the airspace they're operating within. In addition, where airspace restrictions are violated registered identities can be used to associate the operator with the vehicle at the time of the infraction. This creates a traceability which enables remediation of the event to reduce future occurrences. The operator license (and registration) makes sense above a certain weight, performance, or operational profile. There is a common precedence for this structure in other vehicle operations. For instance, to drive your personal vehicle a common state license is appropriate, but for commercial or heavy vehicle operation additional licenses are required due to the increased size, capacity and operational profile. The same exists in traditional aircraft space where separate licenses exist for recreational, visual, instrument, and commercial.

Through the work of the TSFG a vision is being created for a central identity management system which can support the registration of a broader set of air vehicles to include UAVs. UAVs will have the first registration provided by local registration authorities and is envisioned to be part of the production process (similar to traditional aircraft with OEMs). 99% of UAS operations will be 'in country' as is the case with general aviation pilots. As more international support is needed, it is expected to evolve into a more centralize registration/certification. An international registration makes more sense for commercial operations where a vehicle would need to have a central registration for validation and accessibility across international boundaries. An ICAO level registry could serve this purpose as it does for traditional aircraft today. Central registration will also support concepts like remote ID where digitally broadcast registration information can be used by pilots or the public to identify the registration of an operational UAV and its pilot to identify and report wayward operators and their vehicles. In this case the registration works like a digital license plate.

Recommendation: The TSFG needs to develop a solution for digital identities and registration which models what's done today for aircraft & pilot registration. That is to say, digitize the processes aviation already uses today instead of trying to invent new approaches.

Recommendation: Registration number & transponder number should be the same thing for drones. A registration should include:

1. Owner /operator /country of registry, (similar to an IP addr)
2. Manufacturer, Vehicle SN, country of manufacture (asserts compliance to design standards) (similar to TCs in traditional aircraft)

6.2 Operations

With the growth in the UAS market, considerations need to be made for growing operational profiles beyond licensing and registration for vehicles. Remote inspection will no longer require service roads and infrastructure along the way. Air taxi operations will make sense in highly congested areas, such as metropolitan areas. Package delivery will ease carbon productions and road congestion through airborne distribution. Each of these use cases will have a different operational profile. Some may need to enter into controlled airspace while some will be limited to low altitude operations. The operational profile and size of the vehicle will likely dictate who the vehicle and operator need to communicate with and what services/links

they use to communicate. Operations which enter controlled airspace will require communication with airspace controllers to enable them to establish lanes of operation to maintain separation from piloted vehicles. Two way communication may need to be supported to address rerouting or modification of flight plans during execution. For roof inspections and hobby photography below 100 feet, within visual line-of-sight (VLOS), operational communication can be limited to peer-to-peer models, and for some beyond visual line-of-sight (BVLOS) low altitude operations, cellular communication may be sufficient.

As the different use cases and operational profiles define communication profiles they will need to consider the requirements on the communications links which will drive considerations of availability, integrity, and confidentiality in those links. Authority operations (such as police) may require confidentiality, availability will be critical for any operations in controlled airspace, and integrity of links and processing will be required in all cases to ensure vehicles and operators execute flight plans as intended without unauthorized intermediate control (man-in-the-middle).

All of these scenarios need to be thought of and taken into account as regulations are developed for operators and OEMs in developing vehicle capability and operational use cases.

Recommendation: AIA to work through ICCAIA to encourage ICAO to support TSFG, RPAS, and Drone Enable in harmonizing cyber-resiliency and cyber-safety needs. AIA needs to work with the FAA to develop a joint U.S. strategy, and through ICCAIA with other CCAs to develop a harmonized international strategy.

7 Summaries of the AIA Cybersecurity Subcommittee Working Groups

7.1 WG1 Regulatory & Standards

7.1.1 RTCA & EUROCAE

RTCA SC-216 and EUROCAE WG-72 have jointly produced industry standards on airworthiness security process specification, information security guidance, and airworthiness security methods. Plenaries of SC-216/WG-72 in 2020 are virtual due to COVID-19. In addition to the challenge of less contact hours due to transatlantic meeting times, some key members are temporarily unavailable. Three standards are currently in development by these two standards bodies. The standards and their current status is as follows:

- DO-355A/ED-204A: Version A released September of 2020.
- DO-ISEM/ED-ISEM: Structure of new Information Security Event Management (ISEM) document is being discussed. New document should include:
    - Aviation sector specific guidance (rather than copy of NIST documents)
    - Vulnerability Disclosure Program guidance (similar to ISO 29147 and ISO 30111)
    - Discussion on vulnerability management
    - Common taxonomy and scoring for vulnerabilities and reporting in aviation (as MITRE has proposed a CVSS for Healthcare)
- DO-XXX/ED-201A: Chapter by chapter reviews completed jointly by both committees. Most recent activity has been overview of Madrid table top exercise (TTX) results.

Recommendation: *RTCA and EUROCAE should look at ways to simplify the standards with a clear focus on cyber-safety with built in flexibility. Harmonization should continue to be a priority, not only between RTCA and EUROCAE, but between these organizations and other standards organizations like ARINC and SAE as well.*

7.1.2 SAE G-32

SAE G-32 Cyber Physical System Security (CPSS) is moving from supply chain topics to assurance of system, software and hardware. G32A is a cross industry committee, that aims at standardizing requirements, practices, and methods related to cyber physical systems security and create a risk management framework that includes an integrated approach across physical, information, cognitive, and social domains to ensure resilience. There is a risk of overlap with DO-326A/ED-202A and DO-356A/ED-203A. However, G-32 standards will be cross-industry so overlap of guidance will point to DO-326A and DO-356A for aviation. There is also an opportunity with this committee to address and close guidance gaps with respect to security related hardware and software assurance activities to allow easier use of COTS (not specific aviation) components.

Recommendation: *AIA to become more involved in G-32 to ensure gaps in guidance material are being addressed, in particular: security refutation testing, risk assessment for products, risk assessment for organizations, vulnerability and incident ranking, and supply chain assessment and ISMS standard per AIA/ASD proposals*

7.1.3 ASTM F44.50

The ASTM F44.50 Working Group WK56374 has been working on a Standard Practice that provides a method to address Aircraft Systems Information Security Protections (ASISP) related to electronic intrusion & security threats. This practice provides a process to address airworthiness security requirements related to Intentional Unauthorized Electronic Interactions (IUEI) that could exploit vulnerabilities of aircraft systems and networks. Similar to the DO-326A, 356A, 355A suite, this standard has been developed considering Level 1, Level 2, Level 3 and Level 4 normal category airplanes. Final Ballot for this standard practice is expected 4th Quarter of 2020.

As currently written, the standard is intended for traditional Normal Category Aircraft (such as those currently certified under 14 CFR 23 and CS-23). In its initial version, the standard is not intended for advanced air vehicles such as eVTOL or complex operations such as those intended for Advanced Air Mobility. The standard is expected to evolve in concert with two strategic ASTM advisory committees, to ensure the growth of the standard with such activities. For eVTOL vehicles, the ASTM AC433 identifies areas of revision to facilitate standards for these vehicles to be used as a Means of Compliance for these aircraft. For autonomous systems, ASTM AC377 examines autonomy in all aspects of aviation, from small unpiloted autonomous systems, to general aviation aircraft, and into the urban air mobility space.

7.2 WG3 – Supply Chain

Supply chain is a topic of scrutiny for aviation as key organizations such as OEMs and Tier 1 suppliers are improving their security, attackers will use weak links within the supply chain for compromising aviation. This approach has been seen in other industries and the lessons learned there need to be applied for aviation. Aviation has features not seen in other industries that need to be accounted for when securing the supply chain, e.g. much higher interdependency of organizations, very long lifecycle products, and difficulty in updating or changing systems due to prerogative safety needs.

As supply chain is a very large and complex topic, the working group first set out to define it as a set of simpler, discrete problems with individual solutions tailored for each domain. The group identified existing standards that can be used for solving some sub-problems or that can be tailored to provide benefit in an aviation context. The group has also identified which new standards or guidance documents should be produced to aid the activities. The supply chain recommendations are intended to be suitable for organizations that fall under EASA's proposed organizational rules as well as for organizations choosing to secure their supply chain without a regulatory requirement to do so. Due to the nature of the global supply

chain, AIA intends to publish the recommendations jointly with ASD. The two organizations aim to harmonize positions by October 2020 and to publish the Supply Chain Recommendations Report by the end of 2020.

The Working Group has analyzed the current state of certification of cybersecurity as it relates to propulsion units. The group identified that the current Special Conditions apply to Part 25 only and that the FAA's current rulemaking program is aimed at Part 25 only as well. The focus on Part 25 without due consideration of the Type Certificate boundaries to propulsion units (Engines and Propellers) means that the airplane manufacturer is under pressure to provide a statement on the security of the complete aircraft without having access to necessary design data as they are out of scope of the particular Design Approval Holder. The working group has used the rules issued by EASA – utilizing AIA's inputs – to provide recommendations to the FAA on issuing rules to ensure consistent and efficient security of the complete aircraft. This recommendation report will be published by the end of 2020.

7.3 WG4 – Cyber-Safety CAT

The Cyber-Safety Commercial Aviation Team (CSCAT) provides a well-structured aviation cyber safety forum to complement (and become a part of) the existing Commercial Aviation Safety Team with the following:

Vision:

- Data driven risk based collaborative cyber safety decision making.
- US-based response to EASA European Strategic Coordination Platform (ESCP) to address end-to-end aviation cybersecurity and develop actionable plans.
- Partnership amongst aviation industry stakeholders to address evolving aviation environment and new threats to safety, i.e. cybersecurity threats.

Mission: Proactive identification & mitigation of aviation ecosystem cyber safety risks.

Goals:

- Reduce U.S. commercial aviation cyber safety risk.
- Work with international partners to reduce cyber safety risk world-wide.

Outcomes: Identification of risks & actionable ecosystem mitigation recommendations for:

- Best practices, standards & technology development
- Aviation Cyber Safety Incident Communications & Response Plans
- EASA/ESCP Harmonization & ICAO Influence
- Guidance and policy as needed

On March 6th 2019, the key U.S. aviation cybersecurity leaders from industry and the U.S. government met at the AIA Headquarters in Washington DC and agreed to move forward with this U.S. Cyber Safety CAT definition effort. This included the U.S. OEM industry (via the AIA Civil Aviation Cybersecurity Subcommittee) and the U.S. government (including the ACI DHS/FAA/DOD Tri-Chairs, FAA cyber leaders from aircraft/operations/airspace, and other ACI DHS leaders).

Since then, Cyber-Safety CAT has achieved several milestones to include:

- Establishment of the Cyber-Safety CAT Technical Team: The Technical Team choose the Internet Protocol Suite (IPS) Use Case for the first analysis with the goal of making the results available for use

by June 2020 to organizations involved in developing guidance for IPS, i.e. ICAO, ARINC, RTCA, and EUROCAE.

- As the IPS analysis comes to a close, Cyber-Safety CAT is working a Table Top Exercise (TTX) to prioritize potential use case categories for future analysis by the Technical Team.
- As Cyber-Safety CAT matures, more aviation cybersecurity stakeholders are going through the onboarding process to include new members from FAA, industry, operators, Air Line Pilots Association (ALPA), and National Aeronautics and Space Administration (NASA).
- Finally, Cyber-Safety CAT is in discussions with Commercial Aviation Safety Team (CAST) leadership on how these two groups interrelate and inter-operate to address evolving threats to aviation safety, i.e. aviation cyber-safety risks.

***Recommendation**: AIA to continue to work together with aviation cybersecurity stakeholders in maturing Cyber-Safety CAT, as well as collaborate with the E.U. and ESCP as the initiative matures.*

***Recommendation**: AIA to actively participate in TTX for potential use case categories for future analysis to drive the direction Cyber-Safety CAT and focus on high impact use cases.*

***Recommendation**: Regarding how CSCAT recommendations on risk and controls get communicated to standards bodies, CSCAT Safety Risk Assessments (SRAs) need to flow to all applicable standards bodies (e.g. ICAO, RTCA, EUROCAE, AEEC, etc.) at the governance level. Then the overarching bodies need to flow to the correct working groups and committees. The CSCAT data model describes what level of data to share, but does not include how and who to share within the standards bodies. The recommended way forward is to set up a coordination / communication CSCAT subgroup and plan separate from Tech Team. Likewise, the applicable industry standards committees should set up a communication model or plan to consume information out of CSCAT.*

Appendix A: Some Examples of Upcoming Meetings & Events

- Aviation Cybersecurity Initiative (ACI)
  - October 15th Aviation Cyber Initiative Community of Interest Bi-Monthly
  - ACI Summit for November 18th and 19th from 1200-1700 ET
  - December 17th Aviation Cyber Initiative Community of Interest Bi-Monthly
- AEEC General Session – May 2021
- ASD
  - Collaborating on Reports: Propulsion White Paper …
- Aviation Information Analysis and Sharing Center (A-ISAC)
  - September 23rd-24th and 30th A-ISAC Summit – Virtual
- Aviation Sector Coordination Council / Aviation Government Coordination Council (ASCC/AGCC) under CIPAC
- ICCAIA Security Committee
  - September ICCAIA meeting with IATA & Airlines – TBD
- IEEE Aerospace Aviation Systems Panel - Monthly Virtual Meeting
  - Digital Avionic Systems Conference (DASC)
- Integrated Communications Navigation Surveillance (ICNS) Systems – June 2021
- ICAO
  - Secretary Study Group on Cybersecurity (SSGC) – Late Q4 2020
  - Trust Framework Study Group (TFSG)
    - September 29th thru October 1st ICAO TFSG/3 – Virtual
    - March 2021 ICAO TFSG/4 Proposed - ICAO Montreal
  - September 14-18 ICAO Working Group I - Virtual
  - April 13-15 2021 Drone Enabled 2021 with Cyber Focus – Virtual
  - Safety Conference – May 17 to 21
- EASA ESCP – Rulemaking for Part AISS
  - October 15-16
  - November 18-19
  - January 11-12, 2021
  - February 2-3, 2021
- EASA Executive Meeting
  - October 28th
- ECSCG – European Cyber Security for aviation Standards Coordination Group
  - January 26, 2021
  - June 2021
- RTCA / EUROCAE
  - September 14-18 RTCA SC216 / WG 72 Working Group meetings
  - September 28th to Oct 1st RTCA SC 223/ EUROCAE WG 108 - IPS - Virtual
  - October 20th EUROCAE General Assembly
  - December 7-11 RTCA SC216 / WG 72 Working Group meetings

Appendix B: Status of Previous Recommendations

The U.S. and other regions need to show the same industry and government commitment as the E.U. as they form their cybersecurity strategies.	*The Civil Aviation Cybersecurity Subcommittee has been working very closely with key U.S. government partner stakeholders (e.g. FAA, DHS, DoD) to help support and facilitate a common coordinated U.S. aviation position. Examples include: supporting ACI as a recognized industry partner, successfully encouraging observer status and participation from all of these agencies in our AIA Civil Aviation Cybersecurity Subcommittee, and leading the joint establishment the Cyber Safety Commercial Aviation Team for the US.*
Aviation industry organizations should obtain the highest-level executive sponsorship within their business and establish a governing integrity framework to address product cybersecurity.	*C-Suite leaders within the OEMs and supply chain companies are meeting periodically to discuss topics like vulnerability disclosure.*
Aviation industry organizations should define a product cybersecurity policy and appoint a dedicated product cybersecurity leader responsible for implementing and maintaining an effective product cybersecurity program within their organization	*C-Suite leaders for aviation product cybersecurity are being appointed or these responsibilities defined within the OEMs and supply chain companies. Regulations like the emerging E.U. horizontal rule will encourage organizational structures which support security within those organizations.*
Definition and adoption of industry-wide awareness guidance specific to aviation product cybersecurity, building on NIST 800-53A.	*Ongoing, carried out through industry standards participation.*
Aviation industry to standardize on acceptable, independently assessed capability models specific to product cybersecurity.	*AIA drafted a report on supply chain risks this year which addresses this topic.*
Definition and adoption of industry-wide minimum development requirements specific to product cybersecurity including guidance for non-certified systems used in aerospace.	*The work of RTCA SC-216, EURACAE WG-72, and SAE G32 are setting a baseline for systems and component level development to help ensure cyber-resilience.*

Aviation industry organizations should establish and adopt a common incident management and incident response capability specific to product cybersecurity.	*This work is being started through the efforts of SC216 & WG72 through the evolution of DO-355/ED-205, ED-201A and development of a new standard. Major aviation industry members have established product cybersecurity Vulnerability Disclosure Programs to support this work (reference see A-ISAC Summit 2020 Panel).*
Organizations should create processes and utilize technologies that protects sensitive product security data while stored at rest, as well as, in transit. (It is projected that Part AISS and ED-201A will address some of these topics.	*Ongoing*
RTCA and EUROCAE should look at ways to simplify the standards with a clear focus on cyber-safety with built in flexibility. Harmonization should continue to be a priority.	*RTCA and EUROCAE are continuing to work together to harmonize current standards and advance new ones collaboratively.*
Even though higher design assurance systems are expected to have the appropriate security measures and be able to protect themselves, it is recommended to stop the threat sooner and implement security measures at the point of access, regardless of the design assurance level of that point of access, to include security measures in the connecting ground systems.	*The ED/DO security standards and emerging regulations have built the foundation for this need.*
Next update of EFB AC needs broader and more in-depth industry review and input. Encourage the operators (via the regulators and/or industry collaboration) to control the EFBs.	*Ongoing*
AIA should encourage industry and regulatory collaboration to define specific policies and guidelines to be applied to all aircraft software.	*This year the AIA Civil Aviation Cybersecurity Subcommittee published a recommendations report on aircraft software security to address this recommendation, and has worked to establish a new ARINC standards activity in this area.*
Ensure security is considered by this subcommittee and appropriately incorporated into the next revision of ARINC 628. Also ensure there is a cybersecurity focal actively participating in the writing of new upcoming ARINC standards, e.g. Onboard Secure Wi-Fi Network Profile and Media Independent Aircraft Network Communications.	*Ongoing*

Guidance has been identified for EFBs, but it is also needed for the other non-trusted services.	*Ongoing*
Evaluate potential value of security logging requirements at the airplane systems level. Consider evaluation across all connected systems, potentially incorporating additional elements from both AIS and ACD domains, and including the use of existing systems event logs in the context of cybersecurity.	*The emerging ISEM standard from EUROCAE is expected to address this gap.*
Long term plan for WG-72 is to work on a forensics/restoration standard. A means should be explored for how to bring some of this work forward without impacting ISEM timeline.	*Being worked by the standards subgroup*
Consider greater guidance regarding the responsibility of the operator for ongoing log analysis.	*The emerging ISEM standard from EUROCAE is expected to address this gap.*
AIA should be involved with EUROCAE efforts, and work to define an appropriate U.S. forum for better addressing cybersecurity for CNS/ATM systems. Now that RTCA is no longer an advisory committee to the FAA, one possibility is for them to work jointly with EUROCAE on a future revision of ED-205. Another possibility is U.S. guidance on ATM security coming from SAE.	*AIA has continued to support the EUROCAE efforts. To address establishing a U.S. forum for product cybersecurity related CNS/ATM and other safety critical areas, AIA has led the charge in partnership with the FAA, to establish the Cyber Safety Commercial Aviation Team.*
Ensure ED-205A or ED-205 supplement explains assurance levels as they relate to the implementation of security measures; and addresses event monitoring, incident handling, and information sharing to collaborate around incident management in the aviation network as incidents arise.	*Expected in ED205A*
Ensure that ATM future data communications and equipment mandates appropriately address cyber-safety, cybersecurity and cyber-resiliency and have a solid business case.	*ICAO has sponsored the development of the Trusted Framework Study Group (TSFG) to focus on this problem and define architecture, technology, and standards needed to guide it.*
Monitor WG-I activities (including DOCs 10094 & 100095) to help shape ICAO policy level efforts and drive standards developed by ARINC, RTCA, EUROCAE and FAA working groups in the right direction for maximum benefit with appropriate cybersecurity solutions.	*Ongoing*

Understanding and shape IRIS Project requirements for aeronautical safety services over Swift Broadband SATCOM for Europe as they will ultimately apply to all aircraft operating in Europe. Regarding aircraft-ground links, stay involved in standards developed by ARINC.	*Ongoing*
Develop cyber-safety regulations, standards and/or guidance to which all companies are held for maintaining continued airworthiness. This should include monitoring and evaluation of their products for applicable vulnerabilities of their products during the life of the product.	*This need is being addressed through the evolution of new cyber regulations from EASA (and soon the FAA) as well as the harmonized RTCA & EUROCAE cyber standards.*
Develop strategy for rapid identification and resolution for CVEs that affect onboard airplane systems and avionics (patching).	*The AIA Civil Aviation Cybersecurity Subcommittee has established a Cybersecurity Supply Chain Working group, which will shortly be publishing a recommendations report that should propose strategies for addressing this issue.*
Capture necessary incident response processes and activities in DO-xxx/ED-xxx.	*Ongoing*
Utilize draft DO-355A/ED-204A to include this guidance and help the operators write their ANSPs. Provide ANSP guidance on how airlines should handle the log data that the aircraft provides as well as OEM response to log findings. Generate a new standard for OEMs (and perhaps others) to have an ISMS to ensure security is considered in all relevant aspects of design and operation.	*DO-355A/ED-204A has been approved and is planned to be published in Sept 2020.*
A lack of guidance in what should be included in the ICA provided by OEMs and suppliers has led to challenges for the operators in developing the necessary programs to provide adequate supporting processes. A committee (such as A4A) could take up the effort to develop some standard guidance on what should be included in the ICA and the format to convey the information in to be most effective.	*Though ICCAIA, AIA and ASD are working with IATA to develop better understanding of the operator needs as well as educate them on the systems and how they operate.*
Aviation industry to standardize an acceptable return to service policy using inputs from government and intelligence agencies. Engage with standards bodies and regulators to advocate for guidance in this space either through standards or regulations to provide a foundation for this work.	*This is expected as part of the ISEM standard.*

In summary, Industry recommends that end-to-end secured software delivery is implemented for all aircraft (including legacy) and that ARINC establish a standard for secure data loaders (work underway). All data loaders, including those of Field Service Engineers, should be secured appropriately. Industry also recommends establishing a commonality for digital signatures built off the Trust Framework in discussion with ICAO. A more detailed version of these recommendations are being developed concurrent to the publishing of this report.	*The AIA Cybersecurity Subcommittee has developed a whitepaper to summarize the current state of the industry and a consensus recommendation to clarify needs.*
In summary, Industry recommends that an objective-based standard be developed for securing Operational Technology that uses existing standards as a basis. Industry also recommends harmonizing existing standards for identifying fraudulent components into one approach for civil and defense purposes. SAE G-32 Cyber Physical Systems Security committee should be consulted as the primary standards development organization working on supply chain security. A more detailed version of these recommendations are being developed concurrent to the publishing of this report.	*The AIA Cybersecurity Subcommittee has developed a whitepaper to summarize the current state of the industry and a consensus recommendation to clarify needs.*
Review NIST standards available today to identify those which should be referenced in a regulatory or advisory capacity to enhance aviation cybersecurity.	*Ongoing*
Review NIST standards addressing new and evolving technology and the potential cybersecurity impacts. For example, Draft NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.	*Ongoing*
Review ISO standards available today to identify those which should be referenced in a regulatory or advisory capacity to enhance aviation cybersecurity.	*Ongoing*
AIA work with ASD on mapping of cybersecurity and cyber-related industry guidance and activities. ASD is an active member of European Cybersecurity Standards Coordination Group (ECSCG), so AIA should coordinate with ASD to communicate this mapping and present a unified industry voice	*Ongoing*
AIA recommends Aircraft Cybersecurity Initiative (ACI) to take the leadership to form an equivalent organization to what is being done with ECSCG to coordinate the various standards efforts across the U.S. and then coordinate with ECSCG to help ensure collaboration and reduce duplication.	*The ACI Tri-Chairs are giving this proposal consideration.*

AIA to work together with industry and the FAA, while coordinating closely with the Aircraft Cybersecurity Initiative, in establishing and maturing Cyber-Safety CAT, as well as collaborate with the E.U. and ESCP as the initiative matures.	*AIA Civil Aviation Cybersecurity Subcommittee worked with ACI to charter the Cyber Safety Commercial Aviation Team. The team has worked together thru an initial Cyber Safety Use Case (IPS for Safety Services) and is positively influencing the ICAO, RTCA & ARINC product cybersecurity requirements. Initial workshops in the Spring of 2020 to identify the U.S. aviation community's top cyber safety concern areas, and in Fall 2020 will choose the top 3 next cyber safety use cases to evaluate. The CS-CAT is also working with CAST leadership on how to define the future relationship between CAST and CS-CAT.*
Via the ICCAIA (International Coordinating Council of Aerospace Industries Associations), AIA should support and bring our recommendations to the ICAO SSGC (Secretariat Study Group on Cybersecurity) and specifically the four SSGC working groups being formed. AIA currently has representation on SSGC Working Group on Current and Future Air Navigation Systems and SSGC Working Group on Airworthiness**)**	*AIA Civil Aviation Cybersecurity Subcommittee continues to provide inputs to the SSGC via the ICCAIA Security Committee.*
Via the ICCAIA (International Coordinating Council of Aerospace Industries Associations), AIA should support and bring our recommendations to the ICAO Trust Framework Study Group (TFSG) to guide and strengthen the TFSG overall, and support the three working groups.	*AIA Civil Aviation Cybersecurity Subcommittee continues to provide inputs to the TFSG via the ICCAIA Security Committee.*
Establish appropriate policies and standards to support a balanced cybersecurity implementation across the global aviation ecosystem.	*Being worked through participation in the standards committees.*
In addition to the cybersecurity industry guidance and activities discussed in this section, AIA to track new industry guidance in evolving technologies like IoT, RPAS, and Wireless Avionics Intra-Communication (WAIC) systems to ensure there is no cybersecurity gap.	*Ongoing*

The digital development community has created formal approaches that aviation stakeholders can use for modeling threats to (and within systems) through Attack Trees and DFD Threat Models. AIA needs to advocate for the use of these methods in the documentation of systems to help facilitate common language in how we discuss and resolve threats to the aviation ecosystem.	*Ongoing*
Industry stakeholders need to have common language and methodologies for communicating the state of a cyber-attack to manage its advancement and minimize propagation. This can be done via EASA ESCP and the upcoming Cyber-Safety CACASRT. Companies and the aviation community need to be knowledgeable how to utilize the Cyber Kill Chain in prevention and response to protect the aviation ecosystem.	*Ongoing*
Work with standards bodies to define and incorporate a more universally applicable use of trusted & untrusted actors within the aviation ecosystem, and possibly define a detailed specific list of trusted and untrusted actors.	*Ongoing*
Develop/recommend a holistic threat model for the airspace system to help standardize the definition of what information within the system is trusted and what information flows represent a possible threat vector. Doing so will help suppliers and OEMs be more cohesive in the development and management of the systems that make up the NAS.	*Ongoing*
Engage aviation industry stakeholders to define and prioritize cybersecurity risks to be addresses for the aviation ecosystem. Leverage our safety culture and history by establishing a joint government and industry commercial aviation security team, similar to what we did with the Commercial Aviation Safety Team (CAST) which developed an integrated, data-driven strategy to reduce the commercial aviation fatality risk in the United States and promote new government and industry safety initiatives throughout the world. This Cyber-Safety CAT is currently under development.	*AIA Civil Aviation Cybersecurity Subcommittee worked with ACI to charter the Cyber Safety Commercial Aviation Team. The team has worked together thru an initial Cyber Safety Use Case (IPS for Safety Services) and is positively influencing the ICAO, RTCA & ARINC product cybersecurity requirements. We held initial workshops in the Spring of 2020 to identify the U.S. aviation community's top cyber safety concern areas, and in Fall 2020 will choose the top 3 next cyber safety use cases to evaluate. The CS-CAT is also working with CAST Leadership on how to define the future relationship between CAST and CS-CAT.*

Monitor the development of risk management focused working groups to support and encourage leveraging existing standards such as NIST.	*Ongoing*
The government must continue to work toward exchanging more unclassified, relevant threat information with the private sector. This includes methods for sharing actionable unclassified information about known vulnerabilities identified in classified programs.	*Ongoing*
The government needs to review and update the policies regarding clearances within the ISAC community to foster better information sharing and situational awareness.	*Ongoing*
AIA and our aviation industry stakeholders must move rapidly to define, develop, and validate effective Incident Management policies and processes to proactively manage product cybersecurity incidents. Leverage the strengths and expertise of our industry to maintain the cyber safety, cybersecurity, and cyber resiliency of the aerospace industry and strengthen our defenses.	*This need is being addressed through the development of the ISEM standard.*
Leverage existing standards and policies to encourage a system-wide holistic approach by industry participants to strengthen digital systems in the aviation ecosystem for improved the system's cyber-resilience.	*Ongoing*
Leverage DoD investments and developments where possible. A good place for the AIA Civil Aviation Cybersecurity Subcommittee to start will be to coordinate formally with the two AIA DoD focused cybersecurity forums (AIA Cyber Security Committee & Supplier Management Cyber Security Working Group).	*Ongoing*
Work via ICCAIA to express the priority for ICAO to develop new and/or modify existing necessary instruments to treat cyber-attacks on the aviation system as unlawful interference. Express the desire to move forward with the proposed SSGC "Legal" working group at the earliest practical availability.	*AIA is supporting inputs to ICAO via the ICCAIA to the Secretariat Study Group on Cybersecurity who have a Working Group addressing this topic.*

Appendix C: Members & Contributors

AIA Working Group Members

David Almeida	*LS Technologies*	Greg Rice	*Collins Aerospace*
Tim Anstey	*Boeing*	Leslie Riegle	*AIA*
Steve Benham	*GE Aviation*	James Robinson	*Boeing*
Britton, Stephanie	*Bell*	Aloke Roy	*Honeywell*
Brian Connolly	*Boeing*	Stefan Schwindt	*GE Aviation*
Dan Diessner	*Boeing [Chair]*	Jason Shuler	*Astronautics*
Kathleen Finke	*Astronautics Corp. of America*	Sam Singer	*Boeing*
Matt Gomez	*Bell*	Brittany Skelton	*Boeing*
Todd Gould	*Boeing*	Stauffer, Adam	*Bell*
Nicole Jolly	*Booze Allen Hamilton*	Sean Sullivan	*BCA Aviation Security*
Corey Jones	*Boeing*	Ryan Terry	*Lockheed Martin*
Dave Jones	*Astronautics*	Jason Timm	*AIA - Director*
Bret G Lynch	*Pratt & Whitney*	Jeff Troy	*GE Aviation*
Steven Marchegiano	*ADI American Distributors*	Mike Vanguardia	*Boeing*
Tom McGoogan	*Boeing*	Keith Wallace	*LS Technologies*
Jennifer Miosi	*GE Aviation*	Brian Witten	*UTC*
Patrick Morrissey	*Collins Aerospace*	Matthew Winslow	*Gulfstream*
Siobvan Nyikos	*Boeing*	Henry (Hank) Wynsma	*GE Aviation [Vice Chair]*
Eric Ransom	*Bell*	Nathan Wright	*Bell*
Daniel Prince	*GE Aviation*		

Cyber Working Group Guests/Observers:

Mr. Alan Burke	*ACI – DOD Tri Chair*	Samantha Lopresti	*FAA*
Gabe Elkin	*MIT Lincoln Labs*	Steve Ramdeen	*FAA*
Will Gonzalez	*FAA*	Ted Rush	*FAA*
Sidd Gejji	*ACI – FAA Tri Chair*	Rob Segers	*FAA*
Cesar Gomez	*ACI – FAA Team*	Remzi Seker	*ERAU*
Jerry Hancock	*Inmarsat / ASD*	Randy Talley	*ACI - DHS NPPD Tri-Chair*
Brain Hoffman	*ALPA*	Julien Touzeau	*Airbus*
Ayan Islam	*DHS CISA*	Lt Col ERIC D. TRIAS	*ACI - USAF DOD*
Terry Kirk	*Aviation ISAC*	Isidore Venetos	*FAA*
Varun Khanna	*FAA*	Keith Wallace	*FAA*