Civil Aviation Cybersecurity Software Distribution and Dataload Cyber Recommendations Report

AIA Civil Aviation Cybersecurity Subcommittee

Dan Diessner – Chair (The Boeing Company)
Hank Wynsma – Vice-Chair (GE Aviation)

Report Authors:

Todd Gould	Boeing
Julien Touzeau	Airbus
Gil Mulin	Airbus
Paul Hart	A-ISAC
Sean Sullivan	Boeing
David Jones	Astronautics Corp. of America
Mark Heck	Raytheon
Tom McGoogan	Boeing (Cyber Incident Management)
Stefan Schwindt	GE
Jennifer Miosi	GE
Brent Hooker	GE
Curt Bisterfeldt	GE

Summary

Software increasingly controls critical civil aviation functions and secure distribution and loading of the aircraft, ground and space segment software is crucial to ensure safety of aviation. The cyber-security aspects of the aircraft software distribution and dataloading has been analyzed in this report including legacy aircraft and future concepts. This report provides recommendations on securing legacy, current and future aircraft with considerations for implementing increased security in an economically viable manner. The report thus provides short term recommendations for immediate improvements in software security as well as medium- and long-term recommendations to ensure a sustainable, secure aviation ecosystem and to be prepared for future technologies

and uses cases. These recommendations are directed mainly at the generation of standards and will allow AIA to ensure standards are developed and applied appropriately.

1 Aircraft Software Security Case

1.1 Problem Statement

Software – including the firmware code for programmable hardware as well as aviation data and databases – is critical for the safe execution 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. There are also some risks in various civil aviation systems beyond just the aircraft – ground and space elements that may pose or contribute to safety risks due to security.

Tampered software can occur at any stage in the lifecycle of the aviation environment, from generation though delivery and storage up to the loading onto the LRUs and other devices installed on aircraft. The Use Case in this covers all aspects of the software lifecycle except generation of software as generation of safety related software is now covered by Special Conditions by the FAA and upcoming regulations in Europe (see RMT.0648 and NPA 2019-01). Overall supply chain related issues of generation of software are discussed in the AIA Supply Chain Recommendations Report as well as the development standards DO326A/ED202A and DO356A/ED203A.

The lifecycle environment of software in aviation is complex as SW may pass through many intermediate steps and take alternative paths until it reaches its ultimate destination of installation on the aircraft. Figure 1 below provides a simplified illustration of the delivery paths and resting locations of software. The figure shows the flow of software as well as the physical hardware. While other supply chain issues are out of scope of this document, the flow of physical hardware is important as the firmware may be loaded into the physical hardware at any of the stations and/or firmware components provided in parallel with the physical hardware.

Due to the membership of AIA, the recommendations in this report apply to aircraft certified under Part 25/CS-25, Part 29/CS-29, Part 33/CS-P and Part 35/CS-E. These recommendations may apply to aircraft and

parts certified under other sections; however, this requires endorsement by the appropriate industry organizations.

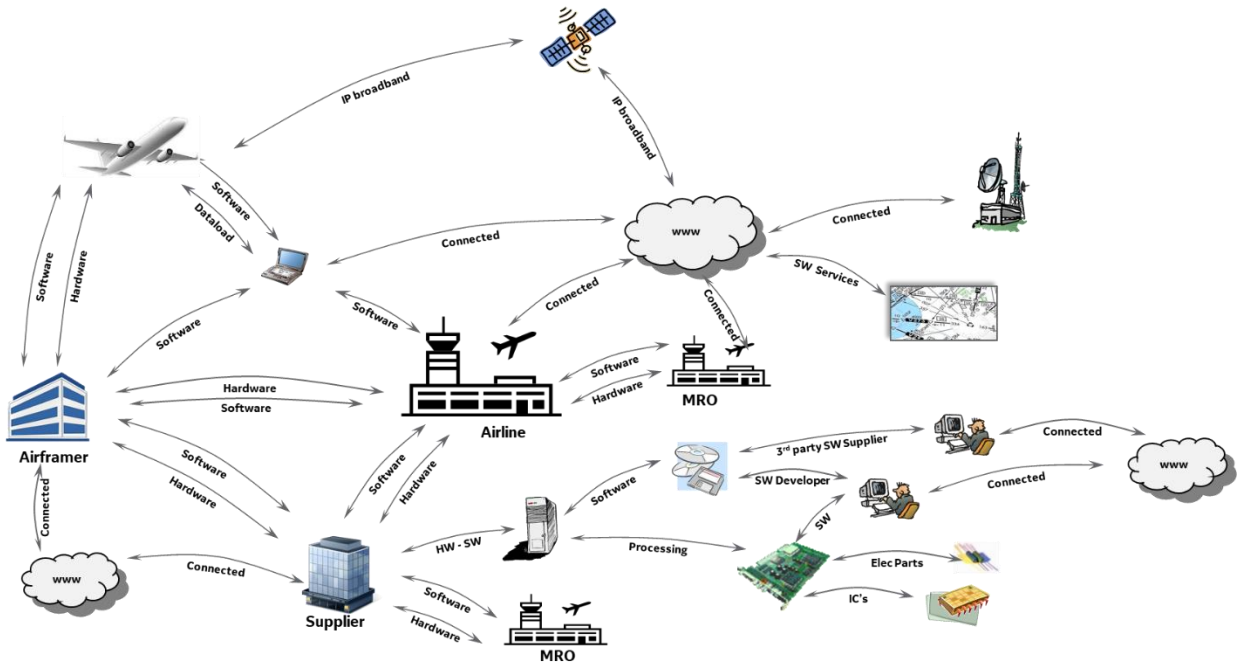

Figure 1: Securing the Aviation Ecosystem

1.2 Current State

Current aircraft include those classified as e-enabled which are defined by the FAA in Order 8900.1 and OpSpec D301 as aircraft using TCP/IP technology for the aircraft backbone connecting flight critical avionics and other systems to essentially make the aircraft an interconnected domain server. The definition of E-enabled includes the capability to reprogram flight critical components via various data transfer mechanisms including wireless means. Current (e-enabled aircraft) have a mix of existing software security mechanisms – to date this has been accepted, but the solutions are somewhat technically and operationally complex and require a fair amount of ongoing IT support to maintain the required PKI and associated tools for signing and verification of signatures. A migration path from current solutions to future solutions is desired to:

- Reduce the cost of security operation for providers and users of software while ensuring security protections remain equal or improve
- Provide for better inter-operability of security mechanisms
- Allow their usage in legacy programs and new generations of manned and unmanned aircraft

Legacy aircraft are secured by non-automated and non-cryptographic means which is error prone. Proposed changes need to consider the nearest fit of security without full redesign. There is no built-in support for cryptography / secure delivery, so it is not easily retrofitted. Technological barriers leading to prohibitive cost should be expected if industry decides to redevelop these aircraft and delivery systems.

1.3 Considerations

Loading of software (and firmware for complex electronic hardware) is an easy and powerful way of changing equipment functionality. Traditionally, airborne electronics have only had protection against installing software corrupted unintentionally (e.g. through errors such as wrong choice of file or random occurrences such as electromagnetic interference) but few protections against intentional/malicious corruption (files crafted to bypass corruption checks and alter equipment behavior). With advent of "e-enabled" (connected) aircraft, Special Conditions require tamper protection security mechanisms as part of the aircraft design. Software deliveries are typically secured from OEM to the aircraft software loader.

Current e-enabled aircraft with Special Conditions are generally well secured but each aircraft OEM uses a unique method and set of tools for software delivery and authentication. Legacy aircraft should be brought (as close as possible) to security of current aircraft. Future aircraft should converge delivery and security mechanisms for economic benefit and additional security.

1.3.1 Non E-Enabled Aircraft (Legacy aircraft)

Federated aviation computers (Line Replaceable Units) – required physical access to each device. LRUs have limited functions and aerospace specific protocols and tools. Some of these are very device specific which would require specific attacks requiring inside knowledge. Many aircraft have a selector switch and ARINC 615 connector which allows a COTS portable data loader (PDL) to load LRUs from a central point. These generally required floppy disk media for loading. Modern PDLs allow other forms of media or network distribution of software. Some aircraft have an airborne data loader (ADL) and required floppy disk for on-board software loading. There are some modernized ADLs that use USB or wireless interfaces. Software was kept only on physical read-only media for several decades. Physical media such as floppy discs are hard to obtain now and have reliability issues. Recently, operators have generally moved away from physical media by storing and distributing software electronically. Centralized maintenance systems including on-board software loaders were developed on several aircraft prior to e-enabled aircraft (e.g. 777). On-board mass storage devices (MSDs) were added to store software for future loads. These aircraft generally still required physical media containing aircraft software to populate the MSD.

1.3.2 E-Enabled Aircraft

E-enabled aircraft are connected to ground systems via broadband IP-based connections and some have networks that are Ethernet-based networks. E-enabled aircraft have on-board software loaders or software loading capabilities with MSDs for software storage. Generally, software can be electronically distributed to these aircraft via portable maintenance devices and/or broadband connectivity links. No specific software security regulations, only issue papers/CRIs negotiated individually. Similar issue papers were applied to these aircraft requiring software tamper protections. E-Enabled aircraft developed independently so solutions vary between OEMs as standards for cyber-security were not available at the time of development. Airbus A380 developed an airplane-wide software cryptographic integrity protection implementation using cryptography and Boeing 787 developed an airplane-wide protection mechanism in parallel. These solutions both use digital signature technology although they are different in implementation. The solutions are documented in ARINC 835.

1.3.3 Challenge of changing current solutions

Various aircraft manufacturers have developed and certified onboard tamper protections on several aircraft models and the cost of change for on-board software is very high if these security mechanisms were to be

changed to have a harmonized solution across the industry. Software that has been changed – whether to update security measures or otherwise – must be re-developed, re-tested, and re-certified for each aircraft model. Aircraft software development is typically 5 times more expensive than typical on ground applications.

The manufacturers have deployed various tools to their software suppliers, production systems, flight, and maintenance operators for each of their solutions. The cost of changing these tools, training suppliers, changing production processes, deploying new operator tools and training operators is very high. In many cases, the operators have integrated software tamper protections with their IT systems security.

Changes to production and operator tools must occur in parallel with airplane software changes (for example so that the signatures and certificates match) and will not disrupt production or in-service operations. It takes operators several months to deploy new software to a fleet of aircraft, so ground tools must support both old and new technologies during the change process and roll to the new process aircraft by aircraft. Months of preparation and testing of the new processes including operational measures and tools will be required by each operator if security mechanisms are changed.

1.3.4 Ultra-high endurance aircraft

The current default position is that it poses a great safety hazard to dataload critical equipment (any equipment with DAL D or higher) during flight as errors or intentional/unintentional corruption could be hazardous to the current flight and that any required updates to the platform of critical equipment – whether for safety or security – can be acceptably delayed until the aircraft lands. This assumption may be true for current passenger aircraft with maximum scheduled flights of around 18 hours and promotional flights of around 22 hours. Beyond work of extending the range of passenger aircraft further – which has limited practical purposes as they are soon able to fly anywhere on the globe – there is work on unpiloted platforms to act as long-term surveillance platforms as well as pseudo satellites. Platforms may be designed with endurance of greater of weeks to theoretically infinite – 2 weeks have already been demonstrated with the Zephyr platform. There will be some value of endurance for which it is no longer acceptable to wait until some high endurance aircraft land before updating the critical equipment as the exposure window can be too high.

1.3.5 Urban Air Mobility and Unmanned Aircraft Systems

The rise of Unmanned Aircraft Systems (UAS) for many use cases including both with passengers (e.g. Urban Air Mobility) and without passengers (e.g. surveying activities) brings many new technological challenges. In terms of software generation, distribution and installation, it currently is not thought that a radical departure from the processes in current piloted large aircraft will take place. The lifecycles may be significantly shorter with less stringent requirements and agile processes but concepts such as only allowing dataloading – which includes significant configuration changes to operational systems and flight controls – during periods when the aircraft is on ground and safe remain true. Nonetheless, it will need to be monitored if any new considerations beyond ultra high endurance aircraft arise and then react accordingly.

2 Recommendations

The overall objective of AIA is to ensure that all aircraft software is protected from tampering end-to-end. In this context, end-to-end means from the supplier generating the software to the aircraft bridging all points in-between in transit and rest. Multiple layers of defense should be applied to protect software tampering in such an end-to-end solution.

Generally, the following three layers should be put in place:

1. Prevent unauthorized access to software via physical and/or electronic access controls;
2. Prevent reverse engineering of software via confidentiality techniques such as encryption;
3. Prevent use of tampered software via integrity and authentication checks.

Definition and agreement of appropriate level of access control, encryption and integrity and authentication will need to be set in industry standards.

As part of the end-to-end security, it is imperative to ensure the integrity of images is preserved such that tampered or un-authentic software can be detected. However, it is strongly recommended that the confidentiality of images is also secured in transit and in rest to make obtaining, reverse engineering and analyzing the software more difficult. As a good practice, all organizations should ensure that systems are correctly secured against unauthorized internal and especially external access.

As the aviation environment is complex with many actors, much regulation, long lifecycles and correspondingly a mix of legacy and new aircraft, the recommendations have been split into near-term objectives to quickly raise the bar on security and longer-term objectives to ensure robust security and a sustainable approach for future technologies and architectures – known and unknown.

2.1 Near-term

The near-term objective is to provide recommendations that leverage existing solutions and technologies to ensure that all actors in the aviation space start to adopt security into their designs to raise the overall security level throughout the industry. In the near-term, competing standards and solutions will be accepted to hasten adoption of solutions by actors currently not securing software or not sufficiently securing software.

Several standards exist already for various aspects of securing software and software deliveries. Thus, the awareness of these standards and their adoption need to be increased.

AIA recommends the following standards or equivalents:

- DO-326A/ED-202A and DO-356A/ED-203A for all new aircraft or for appropriate modifications of legacy aircraft
- DO-355/ED-204 process controls used for all aircraft software
- ARINC 827 for all SW deliveries between companies
- ARINC 835 implemented in all software loaders, software load tools, software storage processes to detect any software tampering.
- ARINC 842 guidance for usage of appropriate digital certificates with use of ARINC 827 and ARINC 835.
- Air Transport Association (ATA) Spec 42

As some of the listed standards have limited scope, AIA will assess limitations of the standards and list further standards in future reports.

These standards provide means for end-to-end security and for modern aircraft with an onboard dataloader and avionics network, full end to end security from loadable software generation to end device is achieved. Security during generation of the software is also a supply chain topic as a secure development environment and trusted supplier is expected – recommendations for the supply chain are provided in the AIA Supply Chain Recommendations Report. However, for legacy aircraft without an onboard dataloader, end to end security can only reasonably be achieved if the offboard dataloader is secured per these standards. This currently is not guaranteed due to a lack of standards providing a common and secure target for offboard dataloaders and a lack of existing standards being levied by regulators or Design Approval Holders (DAH) holders.

- AIA recommends a new common standard for configuring/producing secure software load devices. This has already been tendered to ARINC. Options to consider individually or in combination are:
    - Secure or hardened OS;
    - Limited or restricted use of media ports (e.g. USB, compact flash);
    - Limited connectivity to secure networks only;
    - Attestation to storage server that dataloader is correctly configured (connectivity restricted, operating system patch, anti-malware current and recently run);
    - Authentication of maintenance personnel prior to obtaining dataload packages and deployment to aircraft;
    - Cryptographic capabilities for ensuring integrity of security check functionalities and checking various digital signatures for integrity and decrypting encrypted transfers.
    - Considerations related to maintaining the security level of the Data Loading device throughout its operational lifecycle (e.g. vulnerability management and operational procedures)
    - Nonrepudiation and logging functions to verify, document and triage change actions made
    - Introduce support for zero trust networking for secure distribution and delivery of dataloads across all relevant networks
- The common standard should primarily cover all off board dataloaders including the types used by operators, maintainers as well as field service engineers of OEM and suppliers. The standard is encouraged to be applicable to on board dataloaders to simplify demonstrating security according to DO356A/ED203A for new aircraft or legacy aircraft newly incorporating onboard loaders.
- SW at rest may be at risk, particularly when end to end security has not been established. AIA thus recommends that the secure software management practices of AC 43-216 and DO-355/ED-204 are adopted by all relevant actors. These recommendations provide a combination of solutions that provide a layer that is agnostic to the networks, media, or storage devices used to store and transfer aircraft software via use of digital signature checks or equivalent. Use of secure networks and secure storage devices may be an alternative stop gap but every network and storage device must then be analyzed to ensure end-to-end security. Eventually the use of secure networks, storage devices, confidentiality, and authentication check in software loaders is necessary to achieve a multi-layered defense in depth solution.

Note: ARINC has approved APIM 019-11 to address the recommendations for software load devices in a supplement to ARINC Report 645.

Note: security of software load devices should not apply only to the devices used by operators as part of routine maintenance using well defined dataloading standards (e.g. ARINC 615A) but should also apply to any loading device used outside of a factory setting such as the specialized loaders used by manufacturer's field service engineers that may use non-standard or custom interfaces (e.g. ethernet, RS-232, RS-422, RS-485).

2.2 Mid-term

In the mid-term, the objective is to ensure that common industry-wide solutions are agreed upon such that a sustainable, economically sound secure environment is established. This would include agreeing on standards that ensure reduced cost throughout the environment such as for signing software by developers or controlling software by operators, simple and low-cost upgradeable technology to ensure continued security and a common trust framework so that multiple formats do not need to be supported at high cost and effort by operators.

Initially, the recommendations should be performed on a voluntary basis as the actors in the industry are at different maturity levels. It may be an undue burden to immediately legislate the use of various cryptographic

solutions on companies that have little experience and it may also continue fragmenting the solution as is the current situation. In the mid-term to long-term, the regulations should be updated to require adoption and use of the agreed standards to ensure that all actors ultimately enforce security and secure ecosystem is established protecting aviation. Regulation should be as technology agnostic as possible but sufficient to provide a necessary baseline of comprehensive end-to-end management of software loading threats. A suitable timeline needs to be considered to phase the recommendations from a purely voluntary best practice stance to making the standards part of regulatory materials. The decision for when to update regulations could be based on a mix of pareto principle and maximum deadline: when the first of either 80% of industry voluntarily acts to standards or a set time (e.g. 5 years) has passed, the standards are adopted into regulation.

AIA recommends that industry engages to define a common toolchain and environment for deploying within ARINC 827, 835 and 842 technical standards and DO-355/ED-204 process standards. Suggestions are to utilize work ongoing within the ICAO trust framework to establish aerospace specific Certificate Authorities (CA) for signing dataloads. These CAs should be run as a non-profit organization specifically tailored to aerospace, e.g. use of cryptographic algorithms and expiry time suitable for aerospace lifecycles. Thus, costs are minimized compared to using commercial (Web) CA, common suite of tools can be utilized across supply base such that reuse by suppliers across customers becomes possible and overhead for operators in managing certificates is reduced. This will reduce economic inefficiencies for entire aviation sector and reduce hurdles for adopting good security practices.

Industry should define principles of architecture for an end-to-end protection of the confidentiality, integrity, authenticity, and access of software with the objective to harmonize when and where the verification of security properties should be performed. These principles would serve as a basis for the future 'Secure Software Eco System' which will define 'how' this should be implemented (see next section). The architecture should also allow for protection of the confidentiality of software when desired or necessary.

If industry decides to have signatures for each step of integration or transit to establish chain of custody, the standards need to ensure that signatures from previous steps are not removed upon verification but instead a process of appending signatures for each subsequent step is incorporated and should ensure software is encrypted throughout all transfer and while at rest. Depending on security philosophy, the dataloader can choose to verify each of the signatures or to rely on a primary signature (e.g. operator, OEM or software load generator each of which would be in the signature keyring).

Dataloading devices should also evolve to ensure mutual authentication of the aircraft, the dataloader and the source – as appropriate for the specific architecture. For off-board dataloaders, the dataloader should verify that is connected to the correct aircraft before attempting to dataload as well as establish it is receiving the software loads from the correct repository while simultaneously, the aircraft would verify that the dataloader attempting to connect is a correctly authorized device from the operator. The repository – hosted at the operator or OEM – should verify that only authorized dataloaders attempt to retrieve software loads. Where on-board dataloaders are used, the process would be simplified to mutual authentication of the on-board dataloader with the repository.

Industry should consider means to provide automated updates of flight plans while aircraft are en route. For piloted aircraft, it has become an accepted means to provide new flight plans to the pilots while in the air although it is expected of pilots to verify and validate the new flight plan. In view of desire to enable single pilot operations in the future, a general approach to reduce pilot workload and the opportunity for traffic aware and environmentally adaptive routing, mechanisms for allowing an aircraft to receive a flight plan from the operations center, verify the sender and authenticity of plan and validate it for use on flight need to be developed. In parallel, the same mechanisms can be used to similarly allow unpiloted aerial vehicles – whether with passengers or without – to receive updated flight plans in a secure manner.

2.3 Long-term

The long-term objective is to ensure the complete aviation ecosystem is secure for deployment of software in a manner that is sustainable both in an economic sense as well as capable of adaption and evolution. The ecosystem needs to be upgradeable for security as well as to adapt for future or new uses of airspace and new technologies. Achieving the long-term objectives is only possible if the aviation industry commits to appropriate innovation and research and AIA encourages all members to set up and participate in relevant initiatives.

New Products: industry to collaborate develop a fully secured software deployment eco system by driving end to end security such that from the source where software is developed to the point where it enters the aircraft, tampering can be detected, confidentiality maintained, and proper access is ensured. The development environment for software needs to be secured – recommendations are provided in AIA's Supply Chain Recommendations Report. Agreement must be reached on a common suite for future aircraft/architectures (e.g. software tools, data loaders, certificates, formats, signing tools). This common suite will provide both economic benefits through consistency across aviation as well as increased security using the "many eyes" approach to ensuring proper implementation of cryptography. As this common suite can be a single point of failure should the certificates or algorithms be cracked, sufficient monitoring by industry is necessary to ensure cryptographic best practices are always followed in the suite definition and that algorithms are updated before serious and exploitable flaws are published. The new ecosystem and common suite should be used for all new products to phase out less secure legacy architectures gradually. The future solution needs to be modular such that certification costs when changing cryptographic elements and algorithms (due to weaknesses that may be found) are low or even negligible if possible and that technological evolution and new airspace usage can be accommodated.

Legacy: AIA recommends changes to legacy aircraft only on an as needed basis driven by the risk climate. Any changes to existing processes/procedures need to be cost effective and sustainable for the legacy aviation ecosystem (e.g. software tools, data loaders, process, etc.).

Ultra-high endurance aircraft: With the high endurance values already achieved and also foreseeable, it may no longer be acceptable to wait until an aircraft has landed until software updates are applied and solutions for securing such aircraft are needed. This may include new architectures, protocols and procedures necessary by industry to allow for in-flight updating of flight safety relevant equipment with demonstration of safety and effectiveness as such changes are a radical departure from existing principles.

3 Next Steps

In line with the near-term recommendations and objectives, the first step is to publish recommendations, with cryptographic guidance, to all member companies on phasing out non-secured software transfers between organizations and to avoid non-secured physical media transfers. Also, the operator security process guidance applying to software contained in DO-355/ED-204 should be applied to aircraft software processes. DAH holders should periodically update their Instructions for Continuing Airworthiness (ICA) guidance to ensure these processes are required and keep up with current threat environments. Regulatory agencies should expect ICA guidance for software security in line with DO-355/ED-204 and enforce this guidance with all operators. For legacy aircraft, where ICA does not apply due to lack of applicable provisions in the type certification (e.g. Special Conditions have not been levied on the design), the DAH should issue and regularly update operator security guidance to ensure that rigorous ground processes are followed for aircraft safety where the aircraft does not have type design security measures.

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

Near-term recommendations include the use of existing ARINC standards – listed in section on near-term recommendations – or otherwise using standard secure web protocols such as SSH, SFTP or SSL, access control, and COTS encryption tools if ARINC standards cannot be used.

Subsequently and in parallel, AIA and its members will engage with the various Standards Development Organizations (SDOs) to establish standards for secure dataloaders and to ensure both manufacturers of dataloaders and airlines are involved to ensure an economically viable and secure solution is found. Further engagement with SDOs will include generation of recommendation on the cryptographic solutions that will underpin security in all software solutions. The primary SDO for dataloaders will be ARINC with APIM 019-11 already initiated. RTCA and EUROCAE are engaged in updating the continuing airworthiness guidance to DO-355A/ED-204A to include relevant aspects of this recommendation report.

The industry will also engage with ICAO in the Trust Framework Study Group to provide a common digital identity signing organization and format that meets the unique requirements for long-term software security and level of trust required for aircraft safety at a reasonable cost and an associated Certificate Authority for managing digital identities in aviation.

The industry should also monitor and promote innovation and research that supports the technologies and architectures necessary to implement the recommendations within this report. In particular, research is necessary in digital certificates and cryptographic algorithms to ensure solutions are available for the long lifecycles of aircraft – cryptographic algorithms regularly become deprecated as weaknesses and new attacks are found and there is potential that concepts such as certificates become obsolete and alternatives will be necessary.

3.1 Choosing suitable Standards Development Organization

Multiple Standards Development Organizations are available to aviation and the choice of SDO should consider the expertise available as well as ensure the interests of all affected stakeholders is balanced. The generation of standards also needs to be coordinated to ensure that there is no duplication or redundancy of standards as well as closing any gaps in standardization.

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

4 Appendix

ARINC: Parity between OEMs and Operators, suitable for standards that may drive cost in operations such as with dataloaders. Typically, ARINC standards do not form regulatory material (not AMCs) but are used as "best practices" as part of compliance to regulations as well as standards that are "best practices" for economic sense.

RTCA: Dominated by OEMs although operators are present. Historically, the only US standards organization that provided regulatory material at the request of the FAA. Now a "typical" SDO that can choose to write standards as member organizations request so not all standards need to form regulatory material.

SAE: Dominated by OEMs. Historically, standards that were used as technical best practices that also are used to show compliance to regulations. Some SAE standards later were adopted as regulatory material.

ETSI: Non-aviation specific standard organization in Europe that has a strong expertise in cryptography and other security areas. Standards are published free to use, ETSI would need guidance for aerospace specific topics.

EUROCAE: European SDO that is equivalent and partnered with both RTCA and SAE.

ISO/IEC/CEN/CENELEC: Non-aviation specific standard organization with strong expertise in security management and processes. Standards in Europe are often given an EN title making them legislative material.

NIST: Non-aviation specific standard organization with strong expertise in cryptography and other security areas. Standards are published free to use, NIST has not shown a strong interest to collaborate on standardization for aviation – at least upon Europe's requests.

5 Abbreviations

AC	Advisory Circular
ADL	Airborne Data Loader
AMC	Acceptable Means of Compliance
APIM	ARINC Proposal to Initiate/Modify an ARINC Standard
ATA	Air Transport Association
CA	Certificate Authority
COTS	Commercial Off The Shelf
CS	Certification Specifications
DAH	Design Approval Holder
EASA	European Aviation Safety Agency

FAA	Federal Aviation Administration
ICA	Instructions for Continuing Airworthiness
ICAO	International Civil Aviation Organization
LRU	Line Replaceable Unit
MSD	Mass Storage Device
NIST	National Institute of Standards and Technology
NPA	Notice of Proposed Amendment
OEM	Original Equipment Manufacturer
OS	Operating System
PDL	Portable Data Loader
RMT	Rule Making Task
SDO	Standards Development Organization
UAS	Unmanned Aircraft Systems
USB	Universal Serial Bus

6 List of references

Reference	**Title**
14 CFR Part 25	Airworthiness Standards: Transport Category Airplanes
14 CFR Part 29	Airworthiness Standards: Transport Category Rotorcraft
14 CFR Part 33	Airworthiness Standards: Aircraft Engines
14 CFR Part 35	Airworthiness Standards: Propellers
AC 43-216	Software Management During Aircraft Maintenance
ARINC 615A	Software Data Loader Using Ethernet Interface

Reference	Title
ARINC 827	Electronic Distribution of Software by Crate (EDS Crate)
ARINC 835	Guidance for Security of Loadable Software Parts Using Digital Signatures
ARINC 842	Guidance for Usage of Digital Certificates
ATA Spec 42	Aviation Industry Standards for Digital Information Security
CRI	Certification Review Item
CS-25	Certification Specifications for Large Aeroplanes
CS-29	Certification Specifications for Large Rotorcraft
CS-E	Certification Specifications for Engines
CS-P	Certification Specifications for Propellers
DO-326A	Airworthiness Security Process Specification
DO-355	Information Security Guidance for Continuing Airworthiness
DO-356A	Airworthiness Security Methods and Considerations
ED-202A	Airworthiness Security Process Specification
ED-203A	Airworthiness Security Methods and Considerations
ED-204	Information Security Guidance for Continuing Airworthiness
NPA 2019-01	Aircraft Cybersecurity