Civil Aviation Cybersecurity Supply Chain Recommendations Report

Civil Aviation Cybersecurity Subcommittee

Hank Wynsma – WG Chair (GE Aviation)
Sean Sullivan – WG Vice Chair (The Boeing Company)

Working Group Membership:

Sarah Stern	Boeing
Tom McGoogan	Boeing
Siobvan Nyikos	Boeing
Bill Scofield	Boeing
Nina Vadja	Boeing
Stefan Schwindt	GE
Jon Fitzmaurice	GE
Jo Vann	GE
Larry Nace	L3Harris

Summary

The supply chain of aviation is extremely complex with flow of structural components, hardware, software and data between many organizations. The supply chain includes a high number horizontally – many suppliers to one customer – and vertically – many sub-tier suppliers to each supplier. This situation provides a large surface where the aviation ecosystem can be attacked. This report provides recommendations on how the difficult supply chain topic can be divided into simpler, manageable sub-problems with distinct solutions. For each part of the supply chain, this report provides recommendations on suitable organizational and technical controls.

Executive Summary

The aviation industry faces a multitude of risks from a cybersecurity perspective some of which have seen actively exploited. With the release of the industry standards DO-326A / ED-202A and DO-356A / ED-203A, the cybersecurity of aviation parts and products have the necessary framework to be appropriately secured. However, the overall supply chain has a very large attack surface due to the vectors per individual organization, the need to secure the horizontal supply chain (of many suppliers to an individual organization) and the vertical supply chain (of many tiers of suppliers for a product or service).

The supply chain has not comprehensively been secured as a result of the complexity. A single solution cannot address all the topics nor offer the ability to harmonize and address the breadth and depth of the supply chain. To solve this issue, this report has developed a matrix to split the supply chain problem into more easily manageable subproblems by considering supply chain organizations as specific to aviation versus those that do not follow aviation regulations and practices as well as defining whether the supply chain delivers physical goods. Based on these sub-problems, a number of recommendations have been developed as specific solutions.

The main outcomes are the need for an Aviation Information Security Management System that is flexible to tailor for the size, complexity and risk an organization poses. Such an Aviation ISMS will help comply with anticipated regulations as well as serve the business requirements of a secure supply chain. The key components of an Aviation ISMS are establishing oversight of an organization with a risk assessment identifying interfaces, critical assets and systems and appropriate security. This Aviation ISMS should be auditable by 3rd parties to avoid costly repeat audits with each customer. Within the overall scope of the Aviation ISMS, the security of the Operational Technology used to manufacture components and parts should be addressed in a consistent manner based off ISO/IEC 62443 as well as the information technology assets used to develop, store and deliver non-physical parts and services. Further aspects include vulnerability management and the communication of vulnerabilities throughout the supply chain for assessment and remediation.

The report provides the next steps to implement the recommendations including suggested standards and standards groups for producing published guidance. The recommendations of this report have been provided to the European Cybersecurity for aviation Standards Coordination Group (ECSCG) for consideration.

This report has identified area requiring future development including procurement of general services and appropriate use and security of cloud services in aviation.

Contents

Figures

Tables

1 Aviation Supply Chain

1.1 Problem Statement

The security of the supply chain within aviation poses a great risk as it allows multiple points for malicious actors to subvert the activities of an organization or its products. Attacks can impact both electronic components – the software[1] and firmware[2] of complex electronic hardware (CEH)[3] running in products or powering the servers providing services in addition to the electronic hardware itself – as well as data[4] and non-electronic components such as structural items. Thus, supply chain security can appear to be an indistinct problem in comparison to securing systems in operation – whether these are enterprise systems, servers or electronic components installed on aircraft. The view of supply chain should consider more than just the operational systems but instead include all systems that are used to support the products and operations. Thus design data, e.g. that used to develop or build products as well as industrial or operational data used to produce or operate products are equally to be protected as the data loaded into the aircraft. In addition, the deep supply chains that exist within aviation horizontally – large number of suppliers to a prime contractor – as well as vertically – multiple tiers of suppliers for each prime supplier – introduces a large attack surface. An illustration of the vertical and horizontal supply chain concept is shown in Figure 1.

Figure 1: Illustration of vertical supply chain depth (left) for each OEM and horizontal supply chain breadth at each vertical level (right)

Figure 2 schematically illustrates the complexity and connectivity of the aviation ecosystem with the complex flow of hardware and software items throughout the aviation ecosystem, however it cannot

[1] Software is considered to include all relevant aspects of code such as operating systems, executables, parameter data items, configuration files, databases and other important data files.
[2] Firmware is considered to include all the logic, especially the programmable aspects, of complex electronic hardware such as FPGAs and CPLDs as well as the microcode of processors
[3] Aviation material often uses the term Airborne Electronic Hardware (AEH), e.g. DO-254/ED-80 and AC/AMC 20-152. In this document Complex Electronic Hardware will be used to include components not installed in the aircraft and AEH should be considered to be a subset of CEH.
[4] Data includes all relevant aspects of software including executables, parameter data items, configuration tables databases, operational data including meteorological and cabin data, and maintenance and other manuals

capture the sheer number of suppliers in the vertical and horizontal tiers. Due to this large problem space, it appears daunting and, from observations in community discussions, it typically has discouraged the community from addressing issues in supply chain security more than superficially. However, careful analysis of supply chain security allows the problem space to be divided into smaller subjects each with distinct and approachable solutions that allow for securing of the entire supply chain.

The threats to the supply chain can occur from external actors as well as insider threats. The recommendations of this report generally provide protection against external and internal threats. Some special considerations apply for identifying and preventing insider threats – these are often intrinsically linked to organizational policies and procedures and may be difficult to provide a common baseline across industry. However, the guidance in https://csrc.nist.gov/CSRC/media/Presentations/Mitigating-the-Insider-Threat-Building-a-Secure/images-media/fissea-conference-2012_mahoutchian-and-gelles.pdf provides the basic elements of an insider threat prevention and detection lifecycle and the framework in https://www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework provides a proportionate response to insider threat. Both can be combined with the background screen suggested in Section 2.4 .

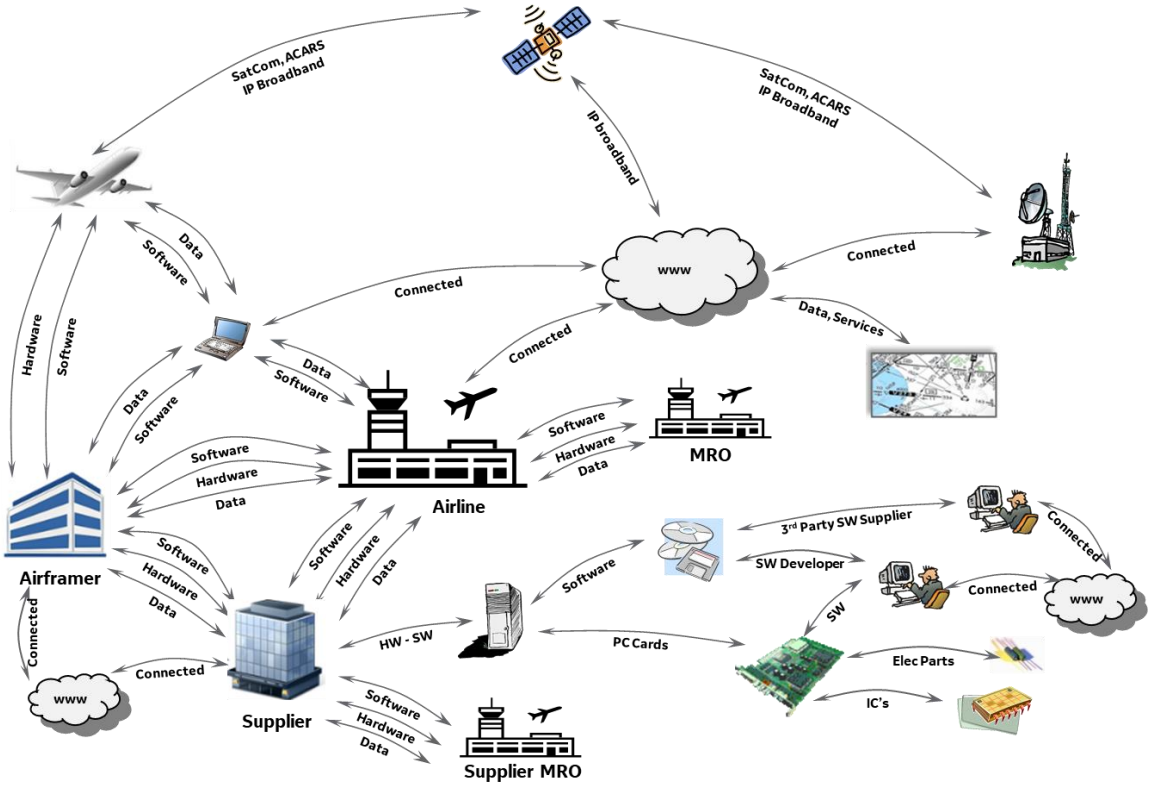

Figure 2: Securing the Aviation Ecosystem

A particular challenge for aviation is finding the appropriate balance between response to security threats and incidents and safety. As a safety critical industry, any change may have repercussions on human lives and traditionally changes are scrutinized to ensure that effects are understood and that no adverse impacts are expected (or at least that the adverse impact is less than leaving the system unchanged). This approach is less effective for cybersecurity where the time between when a vulnerability is identified, a proof of concept for exploits is demonstrated and active exploitation occurs can range from days to even hours. Therefore, systematic and proactive solutions to mitigate vulnerabilities associated to unaccepted risks must increase resilience of individual systems as well as the entire ecosystem and provide multiple layers of defense ensuring they cannot be exploited during the time when reactive countermeasures (e.g. patching of systems) are identified and implemented. These solutions need to be balanced with a continuous and reactive approach.

This report provides recommendations for securing the supply chain in response to upcoming regulations as well as for securing the business interests of all member companies. The proposed regulations for civil aviation are targeted at ensuring continued safe aviation operations whereas business interests

additionally include protecting operations and securing intellectual property. The recommendations within this report principally are intended to secure the manufacturing sector – the organizations involved in designing and producing aircraft, maintenance, repair and overhaul of organizations, and the associated supply chain in supporting those organizations in their activities and supporting air and ground operations of aircraft. However, the recommendations in this report can be applied by all other stakeholders involved in the ground and air operations of aircraft including air traffic management, operators and airports.

1.2 Definition and Identification of Supply Chain Categories

The first step in addressing the supply chain security challenge is defining "the supply chain" and the risks encountered in the facets of the supply chain. For purposes of this document, the supply chain security encompass delivery of physical goods including hardware, structural parts and non-physical goods and services such as software, firmware, data and cloud applications from external companies to an organization. The supply chain also includes internal manufacture[5] of hardware including parts, components and end items as well as the internal development of software. The risks to the supply chain are where subversion can occur through a direct attack on involved systems, system's components or supporting data or the risk of subversion of the information technology and operational technology used to design, manufacture and deliver system's components or supporting data as well as the compromise by persons involved in the physical generation of externally sourced goods and services.

Another issue to be considered is the extent of control and auditing that can be exercised. Where the good or service is aviation specific – e.g. to specific contracts and requirements – there is more control of the supply chain with industry security requirements and performance auditing. However, there is less industry control of requirements and auditing for catalogue items, Commercial / Modified Off-The-Shelf (COTS/MOTS) items and Open Source, that are typically procured from the non-aviation specific supply chain.

This context gives rise to a matrix of issues, as shown in Figure 3. The columns of the matrix show how organizations in the supply chain can be split between actors operating wholly or mainly in the aviation arena and are subject to strong regulatory and commercial pressure to follow aviation industry standards and guidance and suppliers who mainly operate in other industry areas and are not subject to regulatory and/or commercial pressures to adopt aviation practices. The rows of the matrix indicate that the products in the supply chain can be split into physical items where the nature of cyber attacks is typically indirect – such as on the manufacturing equipment producing the physical items or the systems used to design the items – from the non-physical products where cyber attacks may directly alter the product. The grey boxes indicate activities that may already exist in attempting to manage security in the supply chain although with potential limitations of not considering the differences in sectors or opening gaps in securing the entire supply chain.

[5] Internal manufacture is considered as regulations currently cover quality only. Internal manufacture is easily and often outsourced at short notice when demand peaks are met so in-house manufacture may not differ significantly from external manufacture. In-house software and hardware development (including the production of code) is not considered explicitly as this is already governed by regulations

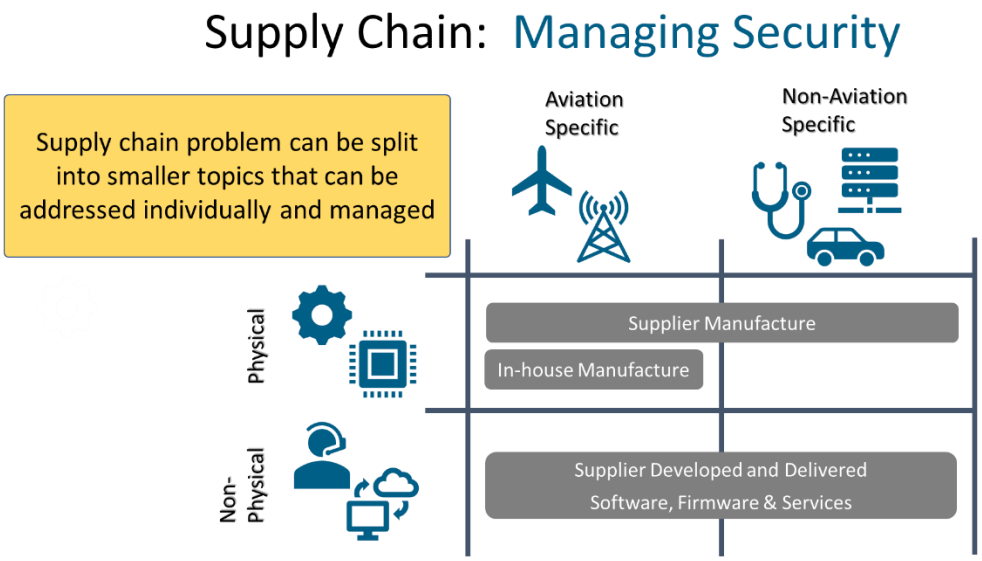

Figure 3: Supply Chain matrix

In the spirit of this matrix, rather than trying to have one set of recommendations to solve all supply chain security concerns, each cell of the matrix will have its own set of recommendations as presented in each Section as follows:

Section 2 provides an analysis of and recommendations for physical goods manufactured specifically for aviation and where auditing is possible.

Section 3 provides an analysis of and recommendations for physical goods procured outside of audit provisions.

Section 4 provides an analysis of the procurement of software developed specifically for aviation.

Section 5 provides an analysis and recommendations for procurement of software outside of audit provisions.

Section 6 provides recommendations on communicating vulnerabilities in the supply chain.

Section 7 provides an analysis of the considerations in establishing trust in the supply chain dependent on relationships.

Section 8 provides an analysis of the need for secure configuration management throughout the supply chain.

Section 9 provide an analysis of the need for an Aviation Information Security Management System to support securing the supply chain and demonstrating security of the supply chain.

Section 10 provides an analysis of procurement of general services.

Section 11 provides an analysis of procurement of cloud services.

1.3 Goals for recommendations to secure supply chain

The complexity of the aviation supply chain brings challenges with each potential solution. Each layer within the supply chain has multiple customers and multiple suppliers. It is not feasible to audit each supplier individually as this would lead to an exponentially increasing number of audits performed and also the undesirable situation that specific processes would have to be tailored for each customer, driving up cost and binding resources for non-value-added activities.

Figure 4 shows the current, undesirable state of supply chain risk management. Specifically, an OEM focused standard and audit scheme with suppliers and their multiple customers would require multiple management processes to satisfy the differing requirements from each OEM or higher tier supplier, which

would be increasingly impractical and costly descending the supply chain and with number of different customers.

With a sub-tier focused approach, each supplier would implement one security process which reduces cost for each individual supplier in contrast to the OEM standard. However, this would increase expense ascending the supply chain as the higher tiers need to resolve different performance in their suppliers with the OEM ultimately needing to harmonize hundreds of different solutions and associated audit overhead.

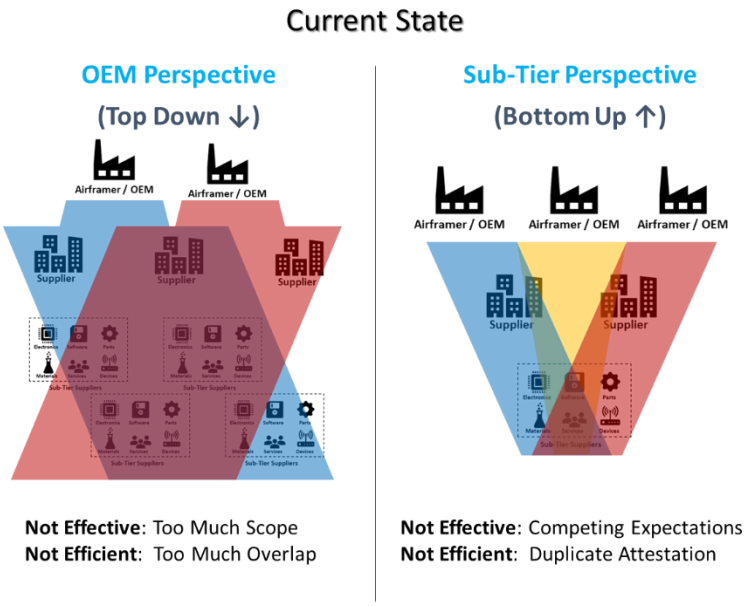

Figure 4: Current auditing and oversight for cybersecurity performance

In order to avoid escalating costs by securing the supply chain, an appropriate concept needs to be established to share responsibility and cost throughout the industry. This can be achieved by establishing a suitable standard and audit scheme, in which all stakeholders in industry would work to an agreed performance level with mutual recognition. The scheme would require an organizational component and a per product component – where the organization lists the security level achieved of the various assets and lists which products utilize the individual assets. This would allow flexibility by suppliers to secure assets at different levels and customers to ensure that their security needs are met. The goals of all recommendations should be to allow for third party audits. With this format, it would be possible for any organization to forgo auditing all suppliers in lieu of visibility of the certification and audit report by a trusted, independent assessor. Any deviations or non-compliances listed in the audit report can be dealt with separately. This solution would allow contracting organizations to reduce the number of audits performed and simplify the audits that need to perform. For suppliers, it allows organizations to establish one best set of processes and procedures that satisfy all customers and reduces the overhead in supplying multiple customers. Such a third-party audit scheme requires consistent requirements and a minimum baseline that meets the needs of all stakeholders. Figure 5 below depicts an industry defined and maintained supply chain risk management approach. An approach using third-party audits in aviation has been successful for quality management activities described in AS/EN/JISQ 9100 and AS 9115, both which are used as partial compliance to Part 21 regulations.

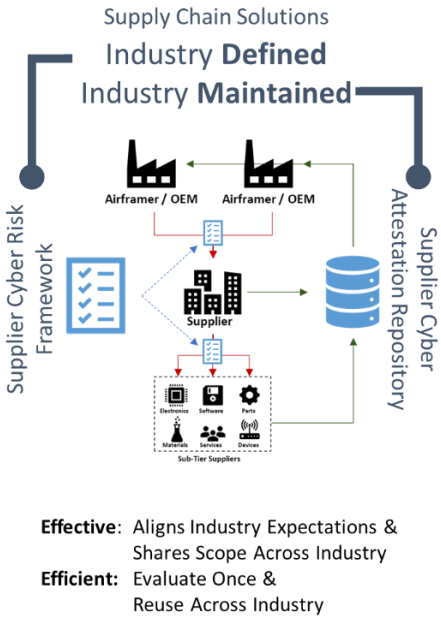

Figure 5: Proposed future auditing and oversight for cybersecurity performance

Existing bodies provide similar schemes for providing industry agreed standards with associated certification schemes. The International Aerospace Quality Group has been established to develop and audit the AS/EN 9100 series quality management systems in aviation. The IECQ/IECEE have been formed to audit the IEC and ISO standards used in a wide range of industries and are currently working on combining several cyber security certification schemes to allow industry maximum flexibility when requesting Third Party audits. For example, IECEE has an IEC 62443 Third Party audit scheme[6] that can be merged with an information security scheme. A new body could also be formed for aviation information security management systems and supply chain security using the IAQG and IECQ/IECEE as a template or either body expanded to include the cybersecurity recommendations of this paper.

Similarly, the goals of the recommendations are to find a means of securing the supply chain that should be satisfactory to both civil and military purposes including dual use equipment. Many products in aviation are directly dual use – they usually can be used unaltered for both purposes – or indirectly – they can be used for military purposes with potential customization or installing supplemental equipment. It already places a burden on companies providing such goods, and it would be of great economic benefit if the dual processes can be minimized.

Ideally, standards and practices can be recommended that are satisfactory for both purposes while minimizing unnecessary costs ensuring that any military specific additional requirements do not require significant changes of processes and procedures – this goal has already been achieved with the aerospace quality standards that have been accepted for military products. Ongoing activities in the military sector involving the Cybersecurity Maturity Model Certification (CMMC) based on NIST SP 800-171 Rev. 2, NIST SP 800-171B (draft), NIST SP 800-53 Rev. 4 and other materials lead in a similar direction to the proposals described in this paper. However, CMMC may be unsuitable in civil aviation as the defense practices are focused on protecting Controlled Unclassified Information (CUI) and Covered Defense Information (CDI) rather than the safety aspects that civil aviation is concerned with opening potential gaps in protection of systems relevant to safety. The CMMC proposals may also drive costs to dual-use items and for small and medium enterprises covered by the proposed regulations compared to the more flexible risk- and effectiveness-based approach recommended in this paper. This is especially true if small and medium enterprises need to achieve higher CMMC levels due to the safety risk of products or services offered by these enterprises.

A proposed solution would be to ensure a suitable standards generation, (including frameworks for coordination and an auditing scheme) include military stakeholders to increase the acceptability of the

[6] https://www.iecee.org/dyn/www/f?p=106:46:0::::FSP_ORG_ID:19409

proposed civil aviation standards for defense purposes. Precedence for this approach exists in the IAQG, which includes the relevant stakeholders, and the AS9100 series standards, which were subsequently accepted for use in defense.

A cybersecurity standards coordination group exists in Europe – the European Cybersecurity for aviation Standards Coordination Group (ECSCG)[7] – which has been tasked with coordinating standards development to prevent redundancy or duplication as well as ensure that standards provide coverage of all topics needed. The ECSCG will not generate or amend any standards but instead will engage with its stakeholders for operational aspects of issuing standards. The ECSCG currently has stakeholders from various industry groups such as ASD for European aviation manufacturers, standards organizations such as SAE, EUROCAE, ETSI, CEN/CENELEC, regulatory stakeholders such as the European Aviation Safety Agency (EASA) and the European Commission as well as the European Defense Agency.

It is recommended that North America establishes an equivalent body to the ECSCG and this initiative is currently being pursued under US ACCESS (US Aviation Coordination of Cybersecurity & E-enabled Standards Strategy). It is further recommended that ECSCG and US ACCESS harmonize to achieve globally accepted standards in both civil and defense – as was for quality management – or alternatively, that North American stakeholders are able to participate in the ECSCG.

The scheme should also establish an Aviation Information Security Management System (ISMS) that is analogous to the Safety Management System that is already mandated. The ISMS would cover the general process aspects such as organization, accountability within the organization, record keeping and training. In addition, the ISMS would provide a consistent means for performing risk assessments of the organization and identifying threats with a common ranking of severity. Based on a standard set of severities, required protection levels are to be defined and applied by the organizations for the systems identified in the risk assessment. For a common trust basis to be established throughout industry and to permit an effective auditing program, the protection levels need to be defined in terms of measurable minimum performance levels. The expectations of how the Aviation ISMS needs to be set up to support supply chain security are discussed in Section 9. The aviation industry is currently considering proposals for an Aviation ISMS to achieve this goal. This proposal for an Aviation ISMS would form the basis of an AMC to Part IS as well as ICAO's International Aviation Trust Framework (IATF) and the ICAO Cyber Security Action plan calling for the guidance on implementation of a Civil Aviation Information Security Management System.

Thus, the ongoing tasks will be to agree on one or more suitable auditing bodies, establishing rules for operation of the auditing bodies, engaging with standards development organizations to implement the recommendations from this document and to validate the recommendations with counterparts from relevant defense bodies.

1.4 Existing regulations and related standards

Many nations have variations of Critical National Infrastructure regulations. The countries define which industries are considered to be critical infrastructure that may either be a particular target of attack or of significant strategic importance to the country and which need protection. Organizations that have been designated as Critical Infrastructure have increased oversight and requirements for cyber and supply chain security. In the US, Presidential Policy Directive 21 and Executive Order 13636 define the transportation sector and certain manufacturing as critical infrastructure. Within the EU, the transportation sector has also been defined to include Operators of Essential Services under the Network and Information System Security (NIS) Directive[8]. In addition, EU Member States have additional Critical National Infrastructure regulations. The approaches between the US and the EU differ as the manufacture of aerospace products and parts has been included in the critical manufacturing sector definition in the US but the NIS Directive applies only to the operators of the infrastructure and do not apply to the manufacturers of the equipment supporting it. As civil aviation not only has an economic impact garnering the focus of most Critical Infrastructure legislation, it also the potential for significant safety impacts. As a result, the

[7] https://eurocae.net/about-us/ecscg/

[8] NIS Directive is published at European Union level in EU 2016/1148. As a Directive, this is transposed into national law for each Member State and specific regulation in each Member State needs to be observed. An implementing regulation exists for Digital Service Providers (DSP) in EU 2018/151

European Commission through EASA is aiming for a holistic approach to secure all organizations in aviation including operators, maintainers, manufacturers and others. Within the US, there is an initiative to monitor and address cyber-safety concerns in aviation under the Cyber-Safety Commercial Aviation Team.

The proposed regulation in Europe is termed Part IS and is part of RMT.0720[9]. It requires any approved organization – including design and production organizations – to assess themselves for cybersecurity risks and put measures in place to secure against the identified risks. The organizations must also consider the interfaces to other organizations and ensure security – either through security measures protecting their interface or extending the security requirements to the interfacing organizations. While the regulation is focused on products and services that have a safety impact[10] to largely field and operational systems, the requirements to consider both organizational interfaces and connected systems, this indirectly requires the approved organizations to consider the supply chain for components, subsystems and other assets. Therefore, the regulation must also address supply chain security as discussed in this recommendation paper.

The FAA currently is not planning for a comparable regulation – although operators do cover aspects through Operational Specifications OpSpec D301 and Advisory Circulars AC 119-1 and AC 43-216. Both EASA and FAA have existing regulations aimed at ensuring safety and quality of produced aircraft that can be extended to include cybersecurity. Nonetheless, AIA recommends that the standards and guidance for supply chain security be followed even in the absence of specific regulations in the respective jurisdictions as supply chain is key to safety and security of the products.

Table 1 Existing civil aviation quality and safety regulations for supply chain

Source	**Title**	**Subject Matter**
14 CFR Part 21.137[11]	Quality System	Provides rules to require control of suppliers such that supplier-provided products, articles or services conform to production approval holder's requirements and that there is a reporting process for non-conformance.
14 CFR Part 21.146[12] 14 CFR Part 21.316 14 CFR Part 21.616	Responsibility of Holder	Requires production, PMA and TSO certificate holders to inform FAA of delegation of authority to suppliers.
21.A.124[13]	Application	Requires evidence of suitability as a production organization. *Note: GM21.A.124(b)(2) requires list of possible suppliers as part of minimum application information.*

[9] NPA 2019-07 lists the proposed regulation as Part AISS (Aeronautical Information System Security). In preparation for the EASA Opinion to the European Commission, the ESCP decided on renaming the proposed regulatory part to Part IS (Information Security)

[10] RMT.0720 does include organizational security requirements for the authorities and these largely mirror the security measures for approved organizations. While the recommendations in this report may also apply to authorities, this report will not consider securing authorities

[11] As current in e-CFR as of May 7, 2020 equivalent to Amendment 21-100

[12] Ibid.

[13] As current in EU 748/2012

Source	Title	Subject Matter
21.A.139[14]	Quality System	Provides rules to require control of suppliers such that supplier-provided products, articles or services conform to production approval holder's requirements and that there is a reporting process for non-conformance. *Note: EASA Part 21 provides Acceptable Means of Compliance and Guidance Material including more detail on surveillance of suppliers similar to the quoted FAA orders*
AC 20-152A / AMC 20-152A[15]	Development Assurance for Airborne Electronic Hardware	Requires applicants to have an Electronic Component Management Plan (ECMP). The plan identifies each commercial hardware part and identifies multiple trusted suppliers/sub-tiers for the part. IEC 62239 and EIA-STD-4899 provide industry standards for preparing such plan.
FAA Order 8120.12A	Production Approval Holder Use of Other Parties to Supplement Their Supplier Control Program	Provides information and guidance concerning use by FAA production approval holders of other-party registered suppliers and contracted other-party supplier surveillance and assessments.
FAA Order 8120.16	Suspected Unapproved Parts Program	Describes responsibilities, policies and procedures for coordinating, investigating and processing FAA suspected unapproved parts reports. Order applies to all personnel involved in the program – including FAA Aircraft Certification Service, FAA Flight Standards Service and FAA Office of Audit and Evaluation.

[14] Ibid.

[15] AMC 20-152A has been issued but the equivalent AC 20-152A has not been issued yet but release is imminent in 2020. See https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/planned/

Source	Title	Subject Matter
FAA Order 8120.23A	Certificate Management of Production Approval Holders	Umbrella document providing guidance on manufacturer's supplier control for all aspects of parts procurement process. It provides guidance and assigns responsibility for the implementation of the Aircraft Certification Service (AIR) certificate management of production activities of manufacturers and their supplier.

For defense companies, regulations apply – most notably DFARS 239.73, 252.246-7007 and -7008. The recommendations made in this paper should be compatible with all civil and military regulations and requirements so as to maximize economic efficiency.

A number of standards exist or are in work that support the supply chain efforts and are listed in the following Table 2:

Table 2 Standards supporting supply chain efforts

Identifier	Title	Subject Matter
DEF STAN 05-135	Avoidance of Counterfeit Materiel	Provides guidance to UK defense suppliers on establishing policy, roles and responsibility and competence for avoiding and identifying counterfeit components with special requirements for suppliers who are manufacturers with a Counterfeit Assurance Maturity Model (CAMM)
IEC 62239-1	Part 1: Preparation and maintenance of an electronic components management plan	Provides guidance and requirements to aviation on establishing an electronic components management plan to choose correct components for intended use and to avoid counterfeit, fraudulent and recycled components
IEC TS 62239-2	Part 2: Preparation and maintenance of an electronic COTS assembly management plan	Provides guidance and requirements to aviation on establishing an electronic COTS assembly management plan to choose correct COTS assembly for intended use and to avoid counterfeit and fraudulent components
IEC 62668-1	Avoiding the use of counterfeit, fraudulent and recycled electronic components	Provides problem statement of counterfeit and recycled statement and guidance to aviation on avoiding such components including audit and accreditation schemes for sourcing from manufacturers and distributors. Supports IEC 62239-1

Identifier	Title	Subject Matter
IEC 62668-2	Managing electronic components from non-franchised sources	Provides extension to IEC TS 62668-1 on sourcing components from non-franchised distributors.
ISO/IEC 20243-1	Open Trusted Technology Provider Standard – Mitigating maliciously tainted and counterfeit products – Part 1: Requirements and recommendations	Provides guidance and requirements to suppliers to demonstrate suitability as a trusted organization and aids customers in demonstrating compliance for supply chain considerations.
ISO/IEC 20243-2	Open Trusted Technology Provider Standard – Mitigating maliciously tainted and counterfeit products – Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018	Provides assessment procedures for auditing organizations according to the Open Trusted Technology Provider standard.
ISO/IEC 27000	Information Security Management Systems – Overview and Vocabulary	Overview document of the ISO/IEC27000 series of documents for establishing a security management system. Series provides general guidance for securing organizations with some sector specific guidance available
ISO/IEC 27036-3	Guidelines for information and communication technology supply chain security	Provides general guidance for securing supply chain related to electronics and extends ISO27000 family with supply chain considerations to satisfy Information Security Management System requirements of ISO27002. Mapping between ISO standards is provided.
IEC 62443-4-1	Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements	Specifies the process requirements for the secure development of products used in industrial automation and control systems. This specification is part of a series of standards that addresses the issue of security for industrial automation and control systems (IACS).
NIST 800-82	Guide to Industrial Control Systems (ICS) Security	Provides general guidance for securing industrial control systems
NIST 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	Provides guidance for US Federal Organizations for securing supply chain based on 3 tier model and links to NIST 800-53

Identifier	Title	Subject Matter
NIST IR 7622	Notional Supply Chain Risk Management Practices for Federal Information Systems	Provides guidance on commercially reasonable supply chain assurance methods and practices.
NIST IR 8149	Developing Trust Frameworks to Support Identity Federations	Provides guidance for trusting digital identities provided by one or more organizations directly or through federation
NIST IR 8183	Cybersecurity Framework Manufacturing Profile	Provides guidance for applying NIST 800-82 in simplified risk framework for manufacturing systems
Draft NIST IR 8276	Key Practices in Cyber Supply Chain Risk Management	Provides key practices in Cyber Supply Chain Risk Management (C-SCRM) to manage cybersecurity risk associated with supply chains.
SAE EIA 993	Requirements for a COTS Assembly Management Plan	Provides guidance to aviation on establishing a management plan for assemblies consisting of COTS parts avoiding use of counterfeit components
SAE ARP 7495	Methods to Address Specific Issues Related to COTS Electronic Components in Airborne Electronic Hardware	Provides more detailed guidance on hardware-related COTS issues and recommendations on existing practices, processes and methods to address them. Methods include additional test and analyses of COTS components beyond supplier tests.
SAE AS 5553	Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition	Provides guidance and requirements to aviation on plans for purchasing electrical, electronic and electromechanical parts
SAE AS 6081	Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors	Provides guidance to aviation on establishing purchasing plans for both purchasing components from distributors
SAE AS 6174	Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel	Provides guidance to aviation on securing supply chain of non-electronic components
SAE AS 6496	Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Authorized/Franchised Distribution	Provides guidance to aviation on establishing purchasing plans for both purchasing components from authorized or franchised distributor and includes specific provisions for military parts.

Identifier	Title	Subject Matter
AS / EN / JISQ 9100	Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations	Provides guidance and requirements on managing processes in a company and ensuring quality audits of adherence to process
SAE AS 9115	Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations - Deliverable Software	Provides supplementary guidance to AS 9100 to ensure software is correctly managed and includes some cybersecurity considerations.
SAE AS 9147 (work in progress)	Unsalvageable Parts Initiative	Provides guidance to avionics OEM with repairs and when to dispose of products to prevent re-entry into the supply chain
SAE EIA STD 4899	Requirements for an Electronic Components Management Plan	Provides guidance and requirements to aviation on establishing an electronic components management plan to choose correct components for intended use and to avoid counterfeit, fraudulent and recycled components

Note: latest standards apply so revisions not listed in this table. Section 14 lists all references quoted in this document including the latest known revisions at time of publication of this document for information.

2 Aviation specific manufacture of physical goods

Aviation specific manufacture of physical goods relates mainly to structural components, assembly of electronic circuit boards and Line Replaceable Units (LRU)s as well as Application-Specific Integrated Circuit chips (ASICs), where these are manufactured in foundries under aerospace control.

2.1 In-house vs. sourced physical goods

The recommendations provided in this section will apply equally to activities performed within the in-house organization as well as the activities performed by an external organization specifically contracted to manufacture the goods. Considerations need to be made when sourcing components to ensure security requirements have been included in the contract clauses and that supplier oversight is ensured – through an independent third-party auditor or through internal audits. The security requirements provided to the suppliers should match those that would exist if done in the home organization and should satisfy all the applicable regulations.

2.2 Securing newly procured Operational Technology

Within the general manufacturing sectors, the need for securing Industrial Control Systems (ICS) and other Operational Technology (OT) has been recognized. As a consequence, the IEC 62443 series of standards has been established that provides guidelines for developing and implementing secure ICS. As any aviation specific design of commodity operational technology, e.g. manufacturing equipment such as Computer Numerical Control (CNC) machines, would come at very high premium, the best course of action would be to leverage the increasing availability of catalogue equipment with security developed to the IEC 62443 standards.

The standards family defines 4 security levels ranging from the lowest security SL1 to the highest security SL4. The standard does not address how to choose security levels other than the type of adversary the security level is intended to be used against. To ensure a level playing field in the market with respect to

regulations as well as ensuring a harmonized level of security, a common strategy choosing security levels is needed.

The recommended approach to achieve this strategy within structural components and electronic assemblies of ICS and other OT is presented in the following paragraphs.

SL4 is developed to protect against nation-state level attackers. For civil aviation, it is thought that there would be no interest for nation state attackers to compromise the manufacture of hardware items – primarily structural items – in a form that is detrimental to safety as nation states and their citizens are users of the civil aviation technologies and they would be unlikely to take precautions to prevent repercussions. In addition, all signatory states of the Chicago Convention on International Civil Aviation (Doc 7300) have committed to refraining from attacks on civil aviation. As SL4 comes at a significant cost premium and equipment to this level is difficult to procure, the decision has been made to adopt a scheme that uses only SL1 to SL3 as such a three tier structure would also map to many risk management frameworks that use a High/Medium/Low approach. This choice of Security Levels would be consistent in not requiring protection against nation state attacker and instead protect from script kiddies to advanced attackers.

However, there are no global nation state commitments to refrain from attacks that disrupt the economy or that steal intellectual property as evidenced by several discovered nation state attacks to obtain technology. All organizations should consider business impact when assigning the security levels for OT equipment. The assigned SL should not be lower than that determined from the safety driven proposals in Table 3 and Table 4. However, where impacts on operations or intellectual property are considered to be greater than the safety impact, higher SL should be assigned.

For structural components, the production of critical components and structures require cybersecurity risk monitoring. The regulations of Part 21[16] only consider primary and secondary structures so a three tier approach can be taken where primary structures are those structures where a failure would have a direct Catastrophic or Hazardous effect and secondary structure are those structures where a Hazardous or Major effect can be expected as there is primary structure that can still withstand relevant loads. All other structures would not carry any significant loads, e.g. cosmetic structures, carpets or acoustic paneling.

For electronic assemblies which would include circuit card assemblies, chassis and complete LRUs, the Design/Development Assurance Level (DAL) of the functions hosted in the device can be used as an analogy. As DAL is a 5-tier system, this would need to be mapped to three levels. One option would be to map DAL A and B to SL3, DAL C and D to SL2 and DAL E (no DAL) to SL1.

As a summary, the proposal for the security levels of machines involved in manufacturing any aviation hardware would be as following:

Table 3 Proposal for Security Level assignment in Operational Technology used to produce structural items

Structural items		
Primary Structure	SL3	Structural items where a failure can lead to a Catastrophic effect with single or multiple failures
Secondary Structure	SL2	Structural items where a failure will have a safety impact

[16] The design parts use different terminology. Part 25/CS-25 uses primary and secondary structure and Part 29/CS-29 uses principal structural element and Part 27/CS-27 uses flight structure. Part 33/CS-E and Part 35/CS-P do not use terminology of primary and secondary structure. Instead, terms used are parts liable to be critically affected and structural components that can lead to a Hazardous Engine Effect. CS-APU uses critical parts. Part 23/CS-23 does not provide any structural classification. For the purposes of these recommendations, terminology of primary/secondary/other structure is used. Each part can use the terminology applicable to part type and using risk assessments map to the definitions in Table 3

Other structures	SL1	Non safety relevant structural items

Table 4 Proposal for Security Level assignment in Operational Technology used to produce electronic components and assemblies

Electronic components and assemblies		
DAL A or DAL B	SL3	LRU, chassis, electronic circuit board, ASIC hosts functions that can directly or in combination cause a Catastrophic effect
DAL C or DAL D	SL2	LRU, chassis, electronic circuit board, ASIC hosts functions cannot cause a Catastrophic effect but will have a safety effect
DAL E	SL1	No safety effect expected from failures

Note: The assignment levels for Security Levels in Table 3 and Table 4 should be considered the minimum levels for a consistent and harmonized approach regarding safety and creating a level playing field within the proposed regulations. Organizations may choose to increase the assigned level to protect business operations or intellectual property according to their internal risk registers.

With this approach, suppliers will only need a minimum of information to choose the appropriate security levels of the manufacturing facilities – only the DAL or structure classification is required. Some manufacturers elect to perform FMECAs of their structures in which case the mapping from DALs can be used as an analogy. This currently cannot be recommended as there are no regulations or acceptable means of compliance requiring this and providing such recommendations in this report would have effects beyond what is intended to be achieved for cybersecurity.

2.3 Securing residual risk of new operational technology and securing legacy OT

It will not be possible to secure all OT based on IEC62443 implementations. This may be from limitations of the standard itself to securing certain types of equipment or architectures, the inability to procure appropriate equipment or use of legacy equipment. Especially the last point cannot be neglected as it would be prohibitive to expect all manufacturers to replace their equipment immediately.

There are several standards from other sectors that offer approaches and solutions for securing organizations. However, many of these have differing disadvantages for use in aviation. Either they are too prescriptive which reduces flexibility for a company to find a solution that has the best cost/benefit ratio and effectiveness for their particular use-case or they are too enterprise focused and do not take into consideration particular aspects of OT environment.

The major standards that could be considered include CIS Top 20 (also captured as ETSI TR 103 305 series), NIST 800-82, the NIST Cybersecurity Framework for Manufacturing (NIST IR 8183) and the ISO 27000 family. NIST 800-82 has a very high number of controls that may be difficult to implement by small or medium organizations and does not provide guidance on the order in which they should be implemented to sensibly mature security capabilities within a company. The NIST Cybersecurity Framework for Manufacturing has provided a means to reduce the high number of controls of 800-82 to make the standard more accessible to smaller organizations but as the NIST standards do not have easily measurable and performance driven controls, the implementation and auditing typically becomes focused on counting controls added rather than effectiveness or performance. The CIS Top 20 and ISO 27000 are

both very objective oriented indicating what goals a company needs to demonstrate to have achieved – by whatever means they consider sufficient and appropriate – and the CIS Top 20 also provides a ranking of more important objectives such that a phased implementation is possible. However, both CIS Top 20 and ISO 27000 are too focused on securing enterprise networks and do not have specific considerations for the OT space, especially the limitations that may exist.

The recommendation from AIA is to establish aviation specific standards for securing enterprise and OT systems in a manner suitable for the aviation environment and the lifecycles that exist in aviation. These standards should form the Aviation ISMS that can be certified for simplified auditing and used as a means of compliance for any future regulations. The design of such an Aviation ISMS is discussed in Section 9.

2.4 Securing manufacturing sites with mixed workforces

A relatively new development in aviation is the existence of manufacturing facilities with inter-corporate workforces, where the employees of other companies may be installing equipment on the premises of another. An example is where the employees of an In-Flight Entertainment (IFE) manufacturer install equipment in the aircraft on the premises of the aircraft OEM. Similarly, it is conceivable that maintenance activities may be performed using staff from separate organizations.

The risk of these working arrangements is that the company accountable for the final project has no means of using their company procedures to vet the foreign employees and may be restricted in other means of ensuring security through processes, procedures and policies. For the accountable organization, they are allowing unknown persons into sensitive areas.

The working arrangements may be very favorable economically to all involved so forbidding these practices is not feasible. Instead, the industry should agree on minimum standards for vetting employees, establishing minimum curriculum for educating manufacturing and maintenance staff in permitted and forbidden activities and zones, establish common means for sharing evidence of vetting and training, and language for inclusion in contracts to establish a legal framework and to allow the accountable organization to direct the foreign workers in any matters within their site. This framework setting common criteria on personnel allowed to interface with the aircraft and associated equipment would allow the OEMs to maintain appropriate oversight of their production lines compliant with regulatory requirements with trust and accountability across organizations supported by authorities.

Further recommendations may be established to increase security including segregating manufacturing and maintenance sites into zones with separate access rights and using color coding for zone and uniform or badges of staff as well as providing separate wired and wireless network access for each organization. OEMs should include the proposed standards for supply chain security into contracts with companies who install equipment, at least until such standards become part of regulatory material.

2.5 Securing design of structural components

The design of structural components does not need specific consideration when installed due to lack of electronic interactions. Supply chain risk is solely restricted to when the design is created and when the design files – used for manufacture – are stored. Design of structural components is done on standard enterprise or enterprise-type equipment which will need to be secured and similarly, the design files will be held in a configuration management system that needs to secure the files during storage and delivery to the OT equipment for manufacture.

Secure configuration management is needed for all design and operational aspects of aircraft and Section 8 discusses the specific aspects of configuration management.

2.6 Securing design and configuration management of complex electronic hardware

In contrast to structural components, complex electronic hardware has electronic interactions when installed in the aircraft and thus the design itself needs to consider security specifically. For the design itself, RTCA DO-356A (ED-203A) has the necessary guidance to ensure security of the complex electronic hardware. DO-356A applies at all levels of aircraft design – aircraft, system and item level – and is invoked in processes from DO-326A (ED-202A). However, the standard does not have a best practice for auditing compliance to DO-356A. For many years, software and hardware (safety) development have had industry

best practices for auditing against DO-178B/C (ED-12B/C) and DO-254 (ED-80) with the Stage of Involvement (SOI) process described in FAA Order 8110.49 and 8110.105. Industry recommends that a similar guide be established as a best practice for ensuring consistent auditing of DO-356A. These best practices can provide guidance on how to reuse audit activities from other areas, e.g. software (DO178B/C / ED-12B/C), hardware (DO-254 / ED-80) and systems (SAE ARP 4754A / ED-79A). The SAE G-32 committee on CyberPhysical System Security (CPSS) is working to address hardware assurance. This activity will not duplicate the work in DO-356A as it will reference DO-356A for the aerospace sector but the CPSS outputs may provide the vehicle for providing the best practice guide for auditing the standard.

Like structural components, the standards for CEH development do not provide requirements for securing the development environment, for example DO-356A / ED-203A only sets objectives for the design of products. It is necessary to secure the assets used for creating the design and configuration management used to hold the design artefacts. This means the principles described in Section 8 apply for the complex electronic hardware development environment as well.

Unlike structural components, the electronic hardware can have vulnerabilities in the fixed hardware and programmable hardware. The development of electronic hardware may also copy external design elements into the fixed or programmable sections, such as COTS IP code. For electronic hardware, the provenance of design needs to be tracked and where portions are derived from non-aviation sectors, the guidance in Section 3 needs to be considered as well as vulnerability management and communication as discussed in Section 6.

While this section discusses CEH, DO-254 may also be applied to other electronic hardware such as Printed Wiring Boards (PWB). While this electronic hardware may not have programmable logic, the design of these components should be protected equally, e.g. the routing and layout of PWB protected by applying the same secure development infrastructure and configuration management principles as for CEH and structural components.

2.7 Establishing supplier trust

As aviation specific suppliers, any issues that affect safety will be detrimental to the suppliers as much as to the higher tier customer(s) and suppliers should have a vested interest in the success of aviation and sharing the burden for securing aviation. As aviation companies, the regulations governing quality and security in aviation will apply to the suppliers and this should bring enforcement of security. Despite this inherent trust, the principle of “trust but verify” should apply and measures taken to establish and continue the trust as described in Section 7.1.

Programmable logic such as COTS IP currently does not make any significant use of the Open Source model that has established itself in the software domain beyond some open architectures such as OpenSPARC and RISC-V. The use of such Open Source hardware components should be considered as non-aviation procured components. However, the aviation industry should monitor developments and risks in using Open Source hardware and issue specific guidance if such components are used.

3 Non-aviation sector manufacture of physical goods

NIST 800-161 noted supply chain risks may include insertion of counterfeit, unauthorized production of, tampering of, theft of components, and insertion of malicious software and hardware, as well as poor manufacturing and development practices in the supply chain. Commercially available solutions present significant benefits for aviation including low cost, interoperability, rapid innovation, a variety of product features, and choice among competing vendors. While commercial off-the-shelf (COTS) solutions can meet the needs of a broad and global base of public and private sector customers; the same globalization and other factors that allow for such benefits also increase the risk of a threat event. These threat events can directly or indirectly affect the supply chain and these risks could remain undetected for extended periods and become undetected risks to end-users who consume these COTS materials in their own integrated solutions.

Where ASICs are manufactured in foundries outside of aerospace control, the manufacture itself should be considered in this category of non-aviation specific manufacture even though the logic design of the ASIC is aviation specific.

The existing standards in Table 2 provide guidance on securing the supply chain of non-aviation specific manufacture of physical goods – these standards should be reviewed and monitored for suitability against known and future cybersecurity risks. Where possible, these standards should be applied on the providers of COTS components. When COTS suppliers do not follow the aviation standards, available evidence should be collected from their respective industries and deviations to aviation standards analyzed. Identified deviations need to be addressed with through suitable measures.

3.1 Components with unknown and undesired functionality

The risks for procuring components is not limited to products of unknown or dubious origin – e.g. counterfeit component acquired from uncontrolled platforms such as eBay or from brokers. Components may be acquired from legitimate sources but have functionality that is either unknown to or undesired by the procurer introducing security risks to the integrated product.

Under NIST 800-161, system integrity is focused on ensuring that the products or services in the supply chain are genuine, unaltered, and that the products and services will perform according to acquirer specifications and without additional unwanted functionality.

DEF STAN 05-135 provides equivalent guidance for the UK Defense industry. Similarly, the suite of IEC standards related to electronic components management plans (IEC 62239-1, IEC TS 62668-1 and 62668-2) and the SAE standards related electronic components management plans (SAE AS 5553C, SAE AS 6081, SAE AS 6496, SAE EIA STD 4899C and SAE ARP 7495) provide aviation specific guidance to ensure that genuine and unaltered components are procured.

However, the main focus of these standards is acquiring components suitable for use case and environment as well as avoiding fraudulent or recycled components. There is little guidance on how to verify authorized components (i.e. from the original manufacturer and not a counterfeit organization) that may maliciously have unwanted functionality. For COTS and other catalogue components, there are few options to audit the supplier due to limitations of the contractual relationship. Consequentially, the industry will have to be selective in the choice of manufacturers and vendors and trust in the organizations that they select. As the only practical defense is trust, a means of monitoring the suppliers needs to be established as well as industry open intelligence sharing to provide early warning and increased resiliency of the aviation sector.

As Intellectual Property (IP) issues prevent merger of the competing standards (IEC and SAE series), AIA recommends that a plan is enacted to harmonize the content of the standards to highest extent and to consider the standards to be equal in compliance to ECMP requirements for standards such as DO254 as well as compliant to supply chain security requirements. It is further recommended that SAE and IEC consider using NIST 800-161 as an input to supply chain standards – however, it should ensure that a flexible and objective based approach is maintained. The standards should also provide guidance on monitoring reputation and behavior of vendors and manufacturers who cannot be audited, monitoring for vulnerabilities and assessing their impact on the systems in which the components are installed and recommending information sharing over various channels throughout the aviation industry. Guidance should also be provided on how to design security around devices that are not fully understood and trusted to protect against unintended events by additional security controls and introducing defense in depth.

Note: SAE has the G-32 committee working on Cyber Physical System Security (CPSS) which can take on these activities. AIA and ASD are jointly developing a proposal for an Aviation ISMS that should address these aspects.

3.2 Components with legacy non-secure protocols or software

Ideally, components with legacy non-secure protocols or software should be avoided. The U.S. Department of Homeland Security (DHS) provides guidance for language to be used in procurement which includes suggested clauses to avoid such a situation and to require reporting by the supplier of any known instances. The guidance may be found at following location: https://www.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf.

If such protocols or software cannot be avoided, for legacy equipment and software, aviation industry organizations must apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems.

Security engineering principles include, for example:

(i) developing layered protections;
(ii) establishing sound security policy, architecture, and controls as the foundation for design;
(iii) incorporating security requirements into the system development life cycle;
(iv) delineating physical and logical security boundaries;
(v) ensuring that system developers are trained on how to build secure software;
(vi) tailoring security controls to meet organizational and operational needs;
(vii) performing threat modelling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and
(viii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

RTCA DO-356A / EUROCAE ED-203A provide guidance for developing architectures that include the security principles described.

3.3 Counterfeit components

Aviation industry organizations must develop and implement effective anti-counterfeit policies and procedures that include the means to detect and prevent counterfeit components from entering the aviation industry equipment and systems. Counterfeit components includes components that have been produced by an unauthorized party and not to specifications, components that are illegitimately sold as a higher specification component, e.g. with a higher environment rating, or components that are not permitted to be resold as they are from an aircraft that has crashed. Some sources of counterfeit software and components include brokers, distributors, manufacturers, developers, vendors, and contractors. Brokers may be considered the highest risk of sources of components, especially when these are not subject to aviation requirements for tracing component lots.

NIST 800-161 and DEF STAN 05-135 provide guidance for defense organizations and both IEC (IEC 62239-1, IEC TS 62668-1 and IEC TS 62668-2) and SAE (SAE AS 5553C, SAE AS 6081, SAE AS 6496 and SAE EIA STD 4899C) provide aviation specific guidance for counterfeit policies. SAE AS 6174A provides additional guidance on detecting and avoiding counterfeit non-electronic material.

Operators and Suppliers must immediately report any detection of counterfeit software and system components to both aviation industry regulatory authorities and original equipment manufacturers per contract requirements. The DHS has provided guidance (https://www.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf) on language to be included in contracts for avoiding, detecting and reporting counterfeit components. Reporting does not need to be in specific formats or using specific tools – encouragement should be made to provide reporting via any means possible to ensure the community is becoming aware. Reporting thus can be via communities such as the A-ISAC or informal means such as an email to the appropriate contacts at a customer or authority. Vulnerability Disclosure Programs should be implemented across the industry and both the aviation and non-aviation supply chain base. For non-aviation companies, ISO 29147 and ISO 30111 provide guidance and language for receiving and managing information on vulnerabilities and incidents as well as notification of customers. For aviation companies, the future RTCA DO-ISEM/EUROCAE ED-ISEM will provide guidance on vulnerability disclosure programs in an aviation environment.

AIA recommends that the standards organizations harmonize the current competing standards or at least mutually recognize them. Further, the standards organizations are encouraged to use the DHS report to suggest procurement language to be used in sourcing as well as encouraging the voluntary sharing of information on counterfeit components and their entry into the supply chain to increase aviation sector resilience. The standards organizations are encouraged to continue to develop anti-counterfeiting policies and procedures support tamper resistance and provide additional levels of protection against the introduction of malicious code.

3.4 Establishing supplier trust

Suppliers from the non-aviation sector cannot typically be audited to the same level that suppliers from the aviation sector can be by virtue of commercial leverage and lack of regulatory enforcement. Nonetheless, aviation relies on such suppliers and measures of trust need to be established to have confidence in the supply chain.

For some physical goods, options do exist for minimum trust of the suppliers as inspection means can be thorough. For raw materials and structural items, it may be feasible to perform thorough inspections and testing to identify any subversions, e.g. crystal structure of bulk metals can be analyzed to ensure correct alloy has been provided. The principles for establishing trust in quality of delivered goods are described in standards such as ISO 9001 and ISO 28958 and may be adopted for assuming a level of trust in delivered goods from suppliers. However, not all testing can be performed in a non-destructive manner – strength testing of materials or structural parts are, by definition, a test of when it fails similarly as testing electrical and electronic components to stress limits. It therefore is a business decision what delivered inwards goods are sacrificed to reach a confidence in suppliers by repeated randomized testing. It may therefore be ultimately cheaper to establish trust in such suppliers using the principles of 7.2 than to solely rely on testing.

For complex electronic hardware, testing is infeasible or impossible as a complete inspection or test of every logic unit and trace in every delivered processor or FPGA requires incomprehensible resources. Thus, customers of such units must establish trust as described in 7.2.

4 Aviation specific SW procurement

The security of software and firmware installed on the aircraft is vital as the majority of critical aircraft functions rely on software and hardware to operate safely especially with increasing connectivity throughout aviation. Where software elements are procured specifically for aviation use, security requirements and audit provisions must be levied on suppliers. Following EASA's update to the Certification Specifications as published in ED Decision 2020/006/R and the FAA expected to be publishing equivalent rule updates to Parts 25, 33 and 35, suppliers should be expected to follow the RTCA DO-326A/EUROCAE ED-202A and RTCA DO-356A/EUROCAE ED-203A standards as part of the development and certification process as well as following the industry recommendations that AIA has published in the 2019 Civil Aviation Cybersecurity Software Distribution and Dataload Cyber Recommendations Report.

4.1 Securing SW design and SW Configuration Management

Software by definition requires electronic interactions and is the main focus when discussing cybersecurity. For the design itself, RTCA DO-356A (ED-203A) has the necessary guidance to ensure security of the complex electronic hardware. DO-356A applies at all levels of aircraft design – aircraft, system and item level – and is invoked in processes from DO-326A (ED-202A). However, the standard does not have a best practice for auditing compliance to DO-356A. For many years, software and hardware (safety) development have had industry best practices for auditing against DO-178B/C (ED-12B/C) and DO-254 (ED-80) with the Stage of Involvement (SOI) process described in FAA Order 8110.49 and 8110.105. Industry recommends that a similar guide be established as a best practice for ensuring consistent auditing of DO-356A. These best practices can provide guidance on how to reuse audit activities from other areas, e.g. software (DO178B/C / ED-12B/C), hardware (DO-254 / ED-80) and systems (SAE ARP 4754A / ED-79A). The SAE G-32 committee on CyberPhysical System Security (CPSS) is working to address software assurance. This activity will not duplicate the work in DO-356A as it will reference DO-356A for the aerospace sector but the CPSS outputs may provide the vehicle for providing the best practice guide for auditing the standard.

The standards for SW development do not provide requirements for securing the development environment, for example DO-356A / ED-203A only sets the objectives for the design of products. It is necessary to secure the assets used for creating the design and configuration management used to hold the design artefacts. This means the principles described in Section 8 apply for the software development environment.

4.2 Software refutation testing

DO-356A / ED-203A has objectives O3.1 to O3.3 requiring refutation testing to demonstrate that delivered items should be free of vulnerabilities and malicious code. However, the standard does not provide specific considerations of refutation testing nor guidance of how to demonstrate compliance to these objectives – it discusses aspects such as fuzz testing but not how to identify if it has been sufficiently thorough. In order to trust and accept software from a vendor, guidance on refutation should be produced to ensure consistent auditing results of developed items.

The term refutation testing was established specifically in DO-356A to describe the testing to refute that an exploitable vulnerability exists in an aviation product. By its nature, refutation testing is negative space testing – attempting to prove that a vulnerability is not present without knowing whether it is present at all. For cost and practicality reasons, the entire negative space cannot be tested so a common understanding on test strategies and procedures needs to be developed by the aviation industry. This would determine the means of approaching the security testing and by what measures it can be considered that testing is sufficiently thorough – the "stop criteria". When these criteria are met, it would be considered that the testing would have reasonably uncovered any vulnerabilities that exist and that an attacker could be expected to find and exploit. Any potential residual vulnerabilities would be deemed acceptable. However, the guidance needs to provide parameters or objectives for demonstrating the quality of testing – a test procedure itself would give attackers a public playbook of what has been tested and where testing has not been performed and an exploitable vulnerability may be found. Some standards suggest setting a fixed time or cost budget for the testing campaign, modelling testing around attacker profiles and assumed proficiency or testing performed by organizations authorized by National Security Agencies. The preferred solution should be using metrics and other measurements that can be objectively assessed to ensure consistent outputs across organizations.

4.3 Delivery of SW

The delivery of software from the organization generating the software through any integrators and operators until it is finally installed on the aircraft is critical. This has been discussed in a separate AIA Software and Dataload Cyber Recommendations Report.[17]

4.4 Establishing supplier trust

As aviation specific suppliers, any issues that affect safety will be detrimental to the suppliers as much as to the higher tier customer(s) and suppliers should have a vested interest in the success of aviation and sharing the burden for securing aviation. As aviation companies, the regulations governing quality and security in aviation will apply to the suppliers and this should bring enforcement of security. Despite this inherent trust, the principle of "trust but verify" should apply and measures taken to establish and continue the trust as described in Section 7.1.

The adaptable nature of software provides additional trust issues. It is possible to take source code from other – potentially untrusted – sources and incorporate it as part of an organization's own product. While such a derived product may be considered to be an aviation specific development or even an in-house developed product, it is crucial to track the provenance of such derived software and to adopt the principles of Section 7.2 for these portions.

5 Non-aviation specific SW procurement

As with hardware, software may be bought as catalogue items from suppliers who will not necessarily provision for audits. The external software can range from source code to libraries and complete binaries. The ephemeral aspect of software introduces another dimension that there may not even be a contractual relationship with the entities creating the software – the rise and success of Open Source Software (OSS) has given many building blocks to be used for which the authors are not known or are barely known and where no form of oversight can ever be performed. The power of some of these collaboratively derived

[17] https://www.aia-aerospace.org/wp-content/uploads/2020/02/AIA-Civil-Aviation-Cybersecurity-SW-Dataload-Distribution-Recommendations-Report-Final.pdf

works, such as the Linux kernel, give foundations that would be prohibitively expensive to replicate under aviation processes so means to continue to allow their use are needed.

As DO-356A cannot be applied (at least in full or for SAL 3) for Open Source Software and certain COTS software, their use should be permitted by augmenting the objectives that can demonstrated with establishing a level of trust, continuous vulnerability management of the used components and performing reasonable inspections of code and binaries. In addition, guidance should be provided on securing around the OSS and COTS software for increasing defense in depth.

The provenance of all external software should be tracked to allow vulnerability management and supplier monitoring.

5.1 Inspections

Vulnerability management should be augmented with various forms of inspection of the code. While it is often infeasible to perform full code reviews of the code being included, a number of tools can be used for various levels of testing. Static code analyzers can be used to identify code snippets that are usually indicative of risk of or actual vulnerabilities and fuzzing tools can be used to dynamically exercise the code to identify issues. Security tools exist for certain packages that can identify misconfigurations and unpatched exploitable vulnerabilities. The refutation testing discussed in Section 4.2 applies to inspections of non-aviation software.

Like vulnerability management, inspections cannot provide absolute security and the two methods augment each other.

5.2 Establishing supplier trust

The final defense with COTS and OSS software is establishing trust in the source using the guidance of Section 7.2. As there is an inherent risk with external software, a good inventory of such software is crucial to all the vulnerability management processes describe in Section 6.1 to be effective

6 Vulnerability Management and Communication

An important factor in all software and complex electronic hardware is managing vulnerabilities as they are discovered and appropriately communicating through the supply chain such that the vulnerabilities can be assessed, remediated and reported.

For enterprise systems, as lifecycles are generally short and the systems are amenable to patching, organizations are expected to implement vulnerability management strategies to quickly address vulnerabilities in enterprise systems. Airborne installations and operational technology have significantly longer lifecycles and it is generally prohibitive to patch regularly or at short notice. The following chapters provide guidance for managing and communicating vulnerabilities in embedded or operational technology systems.

6.1 Vulnerability management in software

Vulnerabilities in custom aviation applications and embedded software, particularly software installed on avionics equipment, may not necessarily be well known and publicized so exploits would be expected to be rare. However, this does not absolve the aviation industry in continuously monitoring for vulnerabilities and communicating findings throughout their supply chain to identify exposure and impact dependent on the implementation of the installed software as well as establishing a suitable update strategy. For aviation specific organization, obligations should be in place to provide reporting of vulnerabilities – see Section 6.3.

Where software is obtained or derived from a non-aviation specific organization, notification of vulnerabilities may not be pushed to the aviation customers – this is particularly the case for Open Source Software. A robust vulnerability management process is essential as vulnerabilities in non-aviation software may be well known and publicized exploits may be available; diligence is required in recognizing these vulnerabilities in used components early and remediating responsibly and responsively. The high

number of vulnerabilities that are captured in databases may make tracking all, identifying applicability to products and patching difficult and each organization will need to determine the scope of products that are included in the monitoring.

Industry recommends establishing a consistent Software Bill of Materials (BOM) format to be used in aviation to ease reporting of installed software in components and communicating higher up the supply chain in further integration. With this Software BOM, vulnerability management can be performed by comparing the installed software with known vulnerabilities received from various sources and tracking resolution of the software updates. The Software BOM should be compatible between the aviation specific software and non-aviation specific software that is incorporate into the aviation products.

It is also recommended for common standards and tool suites to be established that define software and hardware inventories and can match these to vulnerability feeds.

6.2 Vulnerability management in hardware

Hardware may include the physical CEH from non-aviation sources that have vulnerabilities as well as external non-physical design elements from non-aviation sources such as COTS IP code integrated into the hardware design. As described for software in the preceding chapter, the design provenance of physical hardware and hardware logic should be tracked with an appropriate BOM and managed with a vulnerability management system to identify and remediate identified vulnerabilities.

6.3 Vulnerability Communication

To ensure consistent notification of vulnerabilities in software and hardware up the supply chain and to authorities, a common description of vulnerabilities and their exploitability is required. For general software, the Common Vulnerability Scoring System (CVSS) was established to score vulnerabilities and create a Common Vulnerability Enumeration (CVE) to publish a vulnerability and its assumed exploitability and impact. In particular the environment scores are less suited for aviation and an adaptation for aircraft is recommended. Mitre has published a concept for CVSS use in healthcare that can be used as a template for establishing an aviation CVSS. The Information Security Event Management document currently being drafted by RTCA and EUROCAE should establish a common scoring method and thresholds for reporting in the supply chain to ensure consistency across aviation in reporting and resolving vulnerabilities.

7 Establishing supplier trust

The complex nature of software and electronic hardware, especially in combination with its installed firmware, means that testing alone cannot provide absolute guarantee of security and there is no hidden or unwanted behavior. It is essential to establish as much trust as possible in the entities providing software and electronic hardware to provide confidence that no malicious or unintended behavior can be expected in untested areas after integration.

Further, the nature of supply chain is that organizations interact and share risks. As aviation constitutes a system of system, there is a reliance of all partners on each other. Unlike other industries, it is not possible to treat partners as untrusted and/or allow them to fail with internal safeguards as protection. It is therefore necessary to establish common levels of trust throughout the aviation environment and ensure that all participants contribute appropriately.

The upcoming ED-201A standard, which is currently without a document number at RTCA, will provide guidance on sharing risks throughout aviation. The standard will provide guidance on sharing the outputs of risk assessments to allow organizations to have a common means of sharing the risks they consider and protect against as well as the framework for establishing external agreements on sharing the identified risks and responsibilities.

7.1 Trust with aviation suppliers

With aviation specific suppliers, the suppliers have vested interest in the success of aviation – commercially to establish trust in order to continue their revenue streams and regulatory to be permitted to continue operating in the domain. The main aspect to establishing trust in this area is to ensure that all

parties are aware of the applicable regulations and industry standards and guidance. Contractual language and requirements specifications should reference the standards that have been agreed upon and ensure that all suppliers follow the same processes – this theoretically should ensure that any work performed in-house or with a supplier should have similar results. The suppliers should also allow for various forms of auditing – such as test witnessing, review of relevant design artefacts and ensuring that organizational processes are in place and observed.

Auditing does come at a cost and it is also in the interest for all to limit this overhead. For organizational aspects, the proposal of establishing and agreeing an Aviation ISMS provides the benefits of allowing a single trusted party to perform relevant auditing and certification. A customer would only need to verify that an appropriate certificate has been issued and audit the specific aspects for a contract, e.g. that design processes are appropriate for the avionics equipment being delivered. The auditing of DO-356A processes in a supplier provide one major step in establishing this trust – if a supplier is seen to compliantly adhere to the standard and all the outputs of the standard are satisfactory, it may be expected that the delivered product was designed securely.

Nonetheless, this trust can be further increased. Suggestions for increasing levels of trust are shared jointly by all developers involved to establish common goals and understanding of security. In addition, it is recommended that customers find means of monitoring the market for indicators of security issues with a supplier and conversely, suppliers voluntarily establishing programs for sharing information and vulnerabilities may further increase trust. For software, the use of identity trust can further strengthen the delivery of software. NIST IR 8149 discusses establishing trust framework for shared digital identities – this work may be used in the ICAO Trust Framework Working Group to establish a common identity federation for aviation.

Particularly for COTS hardware, ISO/IEC 20243-1 and 20243-2 provide a means for suppliers to provide evidence of good practices such that they can be trusted by customers. These standards are the ISO/IEC implementation of the Open Trusted Technology Provider Standard (O-TTPS) for which a certification scheme exists that has been used in certain defense contexts. The O-TTPS performs its own audit process and database, IEC has not yet stood up the capabilities within IECQ. The standards may not provide all of the aspects necessary for aviation but a modification or supplement to the standard may provide part of the basis for a simple third-party audit scheme for establishing trust in suppliers.

7.2 Trust with non-aviation suppliers

Because aviation software, information systems, and components may often be employed in critical activities and operations impacting flight safety and airworthiness, aviation industry partners have a strong interest in ensuring that these systems remain trustworthy. The degree of trust required needs to be consistent with the design assurance and role that the system/component/service serves and under the conditions for which they are designed to be deployed. With suppliers outside of the aviation space, there is no strong vested interest in supporting aviation standards and audits as they would interfere or raise costs of existing business practices and deny any support. With Open Source, there are no organizations that can be required to follow standards or who can be audited.

AIA recommends establishing standards that provide guidance on monitoring reputation and behavior of vendors and manufacturers who cannot be audited, monitoring for vulnerabilities and assessing their impact on the systems in which the components are installed and recommending information sharing over various channels throughout the aviation industry. If third-party audits and attestation are performed, the results could be held in a database restricted to appropriate organizations. Additionally, communities such as AIA or A-ISAC could generate a lists or databases of preferred or vetted suppliers as well as those that have been found to be in violation or otherwise in loss of trust.

ISO/IEC 20243-1 and 20243-2 provide a means for suppliers to provide evidence of good practices such that they can be trusted by customers. These standards are the ISO/IEC implementation of the Open Trusted Technology Provider Standard (O-TTPS) for which a certification scheme exists that has been used in certain defense contexts. The O-TTPS performs its own audit process and database, IEC has not yet stood up the capabilities within IECQ. The standards may not provide all of the aspects necessary for aviation but a modification or supplement to the standard may provide part of the basis for a simple third-party audit scheme for establishing trust in suppliers.

The Aviation ISMS should consider how evidence provided by suppliers – such as ISO 27001 certification – can be used to establish a level of trust augmented by further specific evidence or mitigations on the contracting side.

8 Secure Configuration Management

The security of configuration management is important as the configuration management system store the design data and non-physical products used in aviation. Any attack on the configuration management systems would allow the design to be altered without discovery leading to hardware being produced with flaws or the delivered software to contain new defects and vulnerabilities. Attacking the configuration management systems also could allow critical IP to be exfiltrated or business operations to be interrupted.

Configuration management systems are not certified systems and usually hosted on COTS systems sometimes with specific aviation solutions. Awareness needs to be raised in organizations of the importance of protecting configuration management systems. The Aviation ISMS should be structured to consider these systems as vital aviation components and demonstrate suitable security.

Some configuration management uses online repositories to store relevant files and outputs. Online or cloud repositories designed for complex development projects with distributed development, such as GitHub, may seem ideal for the globalized structure of aviation. However, the risk of repositories hosted outside of an organizations direct control has significant risks. Attackers continuously attempt, and unfortunately frequently succeed, to find misconfigurations in these repositories such that they can extract code, deface the site, take over repositories or do other damage. Where companies choose to use such services, significant effort needs to be invested in ensuring that the access configurations are correctly set on deployment and that continuous monitoring is in place for changes to server configurations, access control, revocation of access rights for offboarding, data flows to unusual destinations or unusual magnitudes. It is also a frequent occurrence that attackers find private keys that have been stored in the online repositories. As changes in aviation – such as revocation and reissue of product key pairs – require significant time, it is even more damaging if these were to be found in a repository. Organizations should therefore ensure there is continuous monitoring for any data in an online repository that may be a private key.

Another aspect of configuration management is keeping product inventories. As discussed in the previous chapters, it is essential to track provenance of hardware and software and have a vulnerability management system to identify any known vulnerabilities to be able to remediate these. AIA recommends that the configuration management systems include the ability for loading Software Bill of Materials – including information on original source for derived software and firmware – to support the vulnerability management system.

9 Aviation Information Security Management System

An Aviation Information Security Management System provides the framework for establishing all the processes necessary to secure an organization. The typical structure of an ISMS is to perform risk analyses of the organization – analogous to those performed for a product as described in DO-356A / ED-203A – and to implement security controls appropriate for all of the identified risks. The ISMS also provides the processes to monitor that the risk analysis is kept current to organizational needs and threat environment and that the controls have been implemented.

There is a significant body of literature for organizations to secure standard enterprise equipment – some as descriptions of controls only while the most commonly known ISMS is the ISO 27000 series and it its industry sector adaptations. Companies should be free to choose the best fit – however it should be recognized that these standards are written to address the internal risk appetite and as such not generally suitable for the situation in aviation of shared risks. EASA Part IS will introduce requirements for EASA or European NAA approved organizations to demonstrate that the relevant assets have been secured. It is recommended that all companies will follow the Acceptable Means of Compliance (AMC) that are to be established for Part IS. Current discussions suggest that the AMCs will be based off ISO27000 to allow compatibility with non-aviation organizations providing ISO27001 certificates.

The recommendation from AIA is to establish aviation specific standards for securing enterprise and OT systems in a manner suitable for the aviation environment and the lifecycles that exist in aviation. Thus, the new standard should use the knowledge and best practices from the listed standards and achieve following goals:

- Common terminology and risk levels
    - Risk acceptance an aviation industry agreed level and not individual company risk appetites
    - Risk assessment outputs and external agreements for communicating roles, responsibilities and performance to be mutually understandable and agreeable
- Objective based
    - Allows flexibility in implementations while ensuring similar levels of security across organizations
    - Allows future proofing by ensuring continues re-evaluation of solution as technology evolves over long lifecycles in aviation
    - Can be used as an acceptable means of compliance to regulations
- Low number of controls or objectives
    - Number of controls or objectives needs to be manageable by organizations, especially those starting with low maturity
    - Auditing is simplified if number of controls are low and well grouped
- Provision for capability maturity
    - Ranking of objectives and other means of establishing capability maturity to ensure a path for establishing and assessing capability maturity is present, especially for new/low maturity organizations
- Auditable
    - Objectives need to be written in a format such that they can be auditable by external assessor
    - Any risk levels need to be defined in aviation wide scale for compatibility of security

The ISMS needs to focus on some common key areas persistent across most organizations such as configuration management, supplier trust and vulnerability management and communication. It also should provide guidance on how to incorporate evidence from other systems (e.g. ISO27001) and the delta audits necessary as well as how to secure against partial or complete non-compliances of links in the supply chain to the Aviation ISMS.

Note: SAE has the G-32 committee working on Cyber Physical System Security (CPSS) which may take on these activities. AIA and ASD are jointly developing a proposal for an Aviation ISMS that should address these aspects.

10 Procurement of general services

Software and firmware are not the only non-physical products procured within the supply chain. The range of services that fit in this category is very diverse and includes data, e.g. weather or navigation data, communication means, e.g. radio or satellite links, or web presences.

The type of general services and the risks they provide need to be defined and analyzed. No specific recommendations are made at this time other than to establish trust as described in Section 7 and extend existing standards with cyber for penetration into non-aviation markets.

11 Procurement of cloud and similar services

Cloud services are a special topic as they are a hybrid between software and hardware as well as general services and the responsibilities for security can vary on the type of cloud service. Cloud services are starting to be adopted within the aviation ecosystem. The use of cloud services in aviation needs to be further defined. Until this has been done, general best practices for securing clouds – such as material

produced by ENISA (European Union Agency for Cybersecurity) – should be employed to avoid typical pitfalls in securing clouds.

12 Next steps

The recommendations contained within this report have been summarized for clarity and identifying the continuing efforts to put these recommendations in practice. Table 5 lists the major recommendations for further industry reports and standardization activities. Target groups and standards have been proposed and the recommendations for standardization activities have already been shared with the ECSCG for inclusion in the roadmaps. When US ACCESS reaches an operational phase, the recommendations will be submitted for inclusion in the respective roadmap.

Table 5 Recommendation of further recommendation reports and standards

Recommendation	**Target group**	**Target Standard**
Establish an Aviation ISMS including secure configuration management guidance	AIA / ASD ISO / IEC / IECQ	New standard
Establish a certification scheme associated with the Aviation ISMS	AIA / ASD IECQ	N/A
Develop guidance for accepting non-aviation cybersecurity certification and addressing supplier deviations from the Aviation ISMS	AIA / ASD	
Document IEC 62443 Security Level assignment principles in a standard	ISO / IEC / IECQ	New standard
Document detailed guidance for inter-corporate workforces	AIA / ASD	New standard
Document minimum standards for vetting personnel and means of exchanging clearances	AIA / ASD	New standard
Develop and document certification auditing of DO-326A/DO-356A (ED-202A/ED-203A)	SAE G-32 RTCA SC-216 EUROCAE WG-72	New standard or JA6801, JA7496 JA6678
Develop “stop criteria” or objectives for refutation testing	RTCA SC-216 EUROCAE WG-72 SAE G-32	New standard or JA6801, JA7496 JA6678
Develop recommendations for establishing trust in aviation supply chain through common contractual language, specification requirements and auditing approach	AIA / ASD	New document
Continue generating and harmonizing counterfeit and other adverse component guidance	IEC SAE	Various
Develop guidance for components with legacy non-secure protocols or software in aviation	AIA / ASD	New report
Develop guidance for securing COTS components	RTCA SC-216 EUROCAE WG-72 SAE G-32	New standard or JA6801, JA7496 JA6678
Develop recommendations for establishing trust in non-aviation supply chain through use of information sharing groups, CPSS standards for other sectors, O-TTPS standards and delta audits from non-aviation ISMS certification	AIA / ASD	New report
Develop a Software Bill of Materials standard or format for aviation	SAE G-32 RTCA SC-216 EUROCAE WG-72	DO-/ED-ISEM and /or JA6801, JA7496, JA6678
Develop a common scoring and communication means for vulnerabilities in aviation	RTCA SC-216 EUROCAE WG-72	DO-/ED-ISEM and/or JA6801, JA7496, JA6678
Develop a report for securing general services	AIA	New Report

Recommendation	Target group	Target Standard
Develop a report for securing cloud services used in aviation	AIA	New Report

13 Abbreviations

AC	Advisory Circular
AIA	Aerospace Industries Association
A-ISAC	Aviation Information Sharing and Analysis Center
AISS	Aeronautical Information System Security
AMC	Acceptable Means of Compliance
ARP	Aerospace Recommended Practice
AS	Aerospace Standard
ASD	AeroSpace and Defence Industries Association of Europe
ASIC	Application Specific Integrated Circuit
BOM	Bill of Materials
CDI	Covered Defense Information
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CFR	Code of Federal Regulation
CHG	Change
CIS	Center for Internet Security
CNC	Computer Numerical Control
COTS	Commercial-Off-The-Shelf
CMMC	Cybersecurity Maturity Model Certification
CPLD	Complex Programmable Logic Device
CPSS	Cyber Physical System Security
CUI	Covered Unclassified Information
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
DAL	Design/Development Assurance Level
DHS	Department of Homeland Security
DOC	Document

EASA	European Aviation Safety Agency
ECSCG	European Cybersecurity for aviation Standards Coordination Group
ECMP	Electronic Component Management Plan
EEE	Electrical, Electronic and Electromechanical
EIA	Electronic Industries Alliance
EN	European Norm
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FMECA	Failure Mode and Effects Criticality Analysis
FPGA	Field Programmable Gate Array
GM	Guidance Material
HW	Hardware
IAQG	International Aerospace Quality Group
IATF	International Aviation Trust Framework
ICAO	International Civil Aviation Organisation
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IECEE	IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components
IECQ	IEC Quality Assessment System for Electronic Components
IFE	In Flight Entertainment
IR	Internal Report
IR	Industry Recommendations
IS	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization

JIS Q	Japanese Industrial Standards, area division Q (Management System)
LRU	Line Replaceable Unit
MOTS	Modified-Off-The-Shelf
NIS	Network and Information System Security (Directive)
NIST	National Institute of Standards and Technology
NPA	Notice of Proposed Amendment
OEM	Original Equipment Manufacturer
OES	Operators of Essential Services
OpSpec	Operational Specification
OSS	Open Source Software
O-TTPS	Open Trusted Technology Provider Standard
PWB	Printed Wiring Boards
RMT	Rulemaking Task
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automobile Engineers
SAL	Security Assurance Level
SL	Security Level
STD	Standard
SW	Software
TR	Technical Report
TS	Technical Specification
US ACCESS	US Aviation Coordination of Cybersecurity & E-enabled Standards Strategy

14 List of references

The following table provides a list of all references

Reference	**Title**
14 CFR Part 21 Amendment 21-100	Certification Procedures for Products and Articles
AC 20-152A (draft)	Development Assurance for Airborne Electronic Hardware
AC 25-571-1D	Damage Tolerance and Fatigue Evaluation of Structure
AC 43-216	Software Management During Aircraft Maintenance
AC 119-1	Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP)
AIA Software and Dataload Cyber Recommendations Report	Civil Aviation Cybersecurity Software Distribution and Dataload Cyber Recommendations Report
AMC 20-152A	Development Assurance for Airborne Electronic Hardware
Commission Regulation (EU) No 748/2012 *(EASA Part 21)*	Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations
Commission Regulation (EU) 2019/881 *(Cybersecurity Act)*	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
CMMC Version 1.02	Cybersecurity Maturity Model Certification
CVSSv3.1	Common Vulnerability Scoring System version 3.1 Specification Document
DEF STAN 05-135 Issue 2	Avoidance of Counterfeit Materiel
DFARS 239.73	Requirements for information relating to supply chain risk
DFARS 252.246-7007 and -7008	Contractor Counterfeit Electronic Part Detection and Avoidance System

Reference	Title
Directive (EU) 2016/1148 *(NIS Directive)*	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
EASA NPA 2018-09	Regular update of AMC-20:AMC 20-152 on Airborne Electronic Hardware and AMC 20-189 on Management of Open Problem Reports
EASA NPA 2019-07	Management of Information Security Risks
ED Decision 2020/006/R	Executive Director Decision 'Aircraft Cybersecurity'
ETSI TR 103 305 (series) ETSI TR 103 305-1 V3.1.1 ETSI TR 103 305-2 V2.1.1 ETSI TR 103 305-3 V2.1.1 ETSI TR 103 305-4 V2.1.1 ETSI TR 103 305-5 V1.1.1 *(Equivalent to CIS Top 20 with additional guidance)*	Critical Security Controls for Effective Cyber Defence
EUROCAE ED-12B *(equivalent to RTCA DO-178B)*	Software Considerations in Airborne Systems and Equipment Certification
EUROCAE ED-12C *(equivalent to RTCA DO-178C)*	Software Considerations in Airborne Systems and Equipment Certification
EUROCAE ED-202A *(equivalent to RTCA DO-326A)*	Airworthiness Security Process Specification
EUROCAE ED-203A *(equivalent to RTCA DO-356A)*	Airworthiness Security Methods and Considerations
EUROCAE ED-79A *(equivalent to SAE ARP 4754A)*	Guidelines for Development of Civil Aircraft and Systems
EUROCAE ED-80 *(equivalent to DO-254)*	Design Assurance Guidance for Airborne Electronic Hardware
EUROCAE ED-ISEM *(equivalent to RTCA DO-ISEM, reference number not yet issued)*	Information Security Event Management
FAA Order 8110.105A	Simple and Complex Electronic Hardware Approval Guidance
FAA Order 8110.49 Chg 1	Software Approval Guidelines
FAA Order 8120.12A	Production Approval Holder Use of Other Parties to Supplement Their Supplier Control Program
FAA Order 8120.16	Suspected Unapproved Parts Program

Reference	Title
FAA Order 8220.23A	Certificate Management of Production Approval Holders
ICAO Doc 7300/9	Convention on International Civil Aviation
IEC 62239-1:2018	Part 1: Preparation and maintenance of an electronic components management plan
IEC TS 62239-2:2017	Part 2: Preparation and maintenance of an electronic COTS assembly management plan
IEC 62443 (series) IEC TS 62443-1-1:2009 IEC 62443-2-1:2010 IEC TR 62443-2-3:2015 IEC 62443-2-4:2017 IEC TR 62443-3-1:2009 IEC 62443-3-3:2013 IEC 62443-4-1:2018-01 IEC 62443-4-2:2019-02	Industrial communication networks – Network and system security
IEC 62668-1:2019	Avoiding the use of counterfeit, fraudulent and recycled electronic components
IEC 62668-2:2019	Managing electronic components from non-franchised sources
ISO 9001:2015	Quality management systems - Requirements
ISO 27000 (series)	Information technology — Security techniques — Information security management systems
ISO 28590:2017	Sampling procedures for inspection by attributes — Introduction to the ISO 2859 series of standards for sampling for inspection by attributes
ISO/IEC 20243-1:2018	Open Trusted Technology Provider Standard – Mitigating maliciously tainted and counterfeit products – Part 1: Requirements and recommendations
ISO/IEC 20243-2:2018	Open Trusted Technology Provider Standard – Mitigating maliciously tainted and counterfeit products – Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018
ISO/IEC 27000	Information Security Management Systems – Overview and Vocabulary
ISO/IEC 27036-3:2013	Guidelines for information and communication technology supply chain security

Reference	Title
ISO/IEC 29147:2014	Information technology — Security techniques — Vulnerability disclosure
ISO/IEC 30111:2013	Information technology — Security techniques — Vulnerability handling processes
MITRE Case Number 18-2208	Rubric for Applying CVSS to Medical Devices
NIST IR 8149	Developing Trust Frameworks to Support Identity Federations
NIST IR 8183	Cybersecurity Framework Manufacturing Profile
NIST SP 800-53r4	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-171r2	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
NIST SP 800-171B (draft June 2020)	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations - Enhanced Security Requirements for Critical Programs and High Value Assets
Presidential Policy Directive 21	Critical Infrastructure Security and Resilience
RTCA DO-178B *(equivalent to EUROCAE ED-12B)*	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-178C *(equivalent to EUROCAE ED-12C)*	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-254 *(equivalent to EUROCAE ED-80)*	Design Assurance Guidance For Airborne Electronic Hardware
RTCA DO-326A *(equivalent to EUROCAE ED-202A)*	Airworthiness Security Process Specification
RTCA DO-356A *(equivalent to EUROCAE ED-203A)*	Airworthiness Security Methods and Considerations
RTCA DO-ISEM *(equivalent to EUROCAE ED-ISEM, reference number not yet issued)*	Information Security Event Management
SAE ARP 4754A *(equivalent to EUROCAE ED-79A)*	Guidelines for Development of Civil Aircraft and Systems
SAE ARP 7495	Methods to Address Specific Issues Related to COTS Electronic Components in Airborne Electronic Hardware
SAE AS 5553C	Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition

Reference	Title
SAE AS 6081	Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors
SAE AS 6174A	Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel
SAE AS 6496	Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Authorized/Franchised Distribution
SAE AS 9100D	Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations
SAE AS 9147	Unsalvageable Parts Initiative
SAE AS 9115A	Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations - Deliverable Software
SAE EIA 993B	Requirements for a COTS Assembly Management Plan
SAE EIA STD 4899C	Requirements for an Electronic Components Management Plan