Civil Aviation Supply Chain Cybersecurity Recommendations Report

Civil Aviation Cybersecurity Subcommittee

Stefan Schwindt– WG Chair (GE Aviation)

Working Group Membership:

Mike Tumminelli	Gulfstream (WG Chair)
Kathleen Finke	Astronautics
Siobvan Nyikos	Boeing
Tom McGoogan	Boeing
John Bush	Boeing
Kanwal Reen	Collins Aerospace
Jayson Clifford	Embry-Riddle Aeronautical University
Lauren Warner	Embry-Riddle Aeronautical University
Stefan Schwindt	GE Aerospace
Larry Nace	L3Harris
David Almeida	LT Tech

October 2023

Summary

The Civil aviation supply chain is extremely complex with flow of structural components, hardware, software and data between many organizations. From the first version of this white paper, the context has changed significantly across the globe. As new legislation and standards are released, and with the level of attention, direct attacks on the aviation supply chain has increased exponentially over the past few years.

While Civil Aviation has long worked to build up and protect its supply chain, the context we face going forward includes both new and pending requirements from the government to improve the security and resiliency of our supply chain. This includes two recent executive orders 14014, "America's Supply Chains" and 14028, "Improving the Nation's Cybersecurity," as well as a new National Cybersecurity Strategy. Among other pending changes, the impact of new industry standards as well as SBOM (Software Bill of Materials) are discussed and contextualized in the various aviation domains.

The paper also identifies a more comprehensive set of direct threats to the civil aviation sector and its supply chain, that are increasing due to growing HW/SW vulnerabilities, insufficient vetting of suppliers, and global access to aviation components and software infrastructures.

Executive Summary

The Civil Aviation Industry and its supply chain partners continuously face a multitude of cybersecurity threats actively attempting to gain access and exploit the aviation industry across its business operations (both large and small), manufacturing processes, and its most critical aviation products and services.

As stated in executive order 14017, "America's Supply Chain" (Feb 2021); "The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. 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 secured.

However, the supply chain that supports civil aviation has a very large and global attack surface with many unique and shared attack vectors. In addition to this immense attack surface, industry experts have noted a sharp increase in ransomware and other attacks to the aviation industry. As cited in a recent Aviation Week article, "Cybersecurity Threats to Aviation Bolstered by Efficiency, Geopolitics", Boeing's CISO Richard Puckett noted in a conference that "occurrences of ransomware inside the aviation supply chain are up 600% in just one year"—as an indicator of escalating cybersecurity risks the industry is facing."

To respond to these increasing threats, AIA considers the current civil aviation supply chain must be viewed not only from its incredible complexity (as a typical commercial airplane could have over 25,000 suppliers), but also from the standpoint of the significant increase in threat attacks across our sector supply chain from the smallest supplier to the largest Original Equipment Manufacturers (OEMs).

It is clear that a single solution cannot address all these concerns nor offer the ability to harmonize across all the regulatory guidance and industry standards needed to address the breadth and depth of our supply chain.

As such, the AIA Civil Aviation Cybersecurity Subcommittee and its government and industry partners has derived the following objectives for improving the safety, security, and resilience of the aviation supply chain to meet these goals:

- Develop guidance for minimum requirements for cyber supply chain risk management
    - Cyber supply chain risk management for organization
        - Cybersecurity as part of the supplier onboarding and supplier certifications
    - Flow down of cybersecurity related requirements to the suppliers
        - Identified according to the kinds of supplier
        - Vulnerability Management program
        - Incident Response
    - Supplier enablement
        - Develop recommendations for using a common framework to assess cybersecurity posture of the supply chain. Encourage use of SBoMs to better identify SW risks and facilitate vulnerability management and incident responses within the civil aviation software supply chain.

In addition to our civil aviation industry partners, recommendations proceeding this report will be provided also to the Federal Aviation Administration and the European Cybersecurity for Aviation Standards Coordination Group (ECSCG) to aid in the development of regulatory guidance and industry standards.

Contents

Figures

Tables

1 Aviation Supply Chain

1.1 Problem Statement

Civil Aviation has an enormously complex and globally connected supply chain. As such, civil aviation's supply chain continuously poses a great risk to the security of the aviation industry as it allows multiple points for malicious actors, including both externally motivated and insider threats, to subvert the activities of an organization for its products and services.

Across aviation, attacks can impact nearly everything in the supply chain, from the data used to build physical structures, to the 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 the data[4] and production systems used to manufacture 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.

As executive order 14017 America's Supply Chain (Feb 2021) noted; "Resilient American supply chains will revitalize and rebuild domestic manufacturing capacity, maintain America's competitive edge in research and development, and create well-paying jobs. …resilient supply chains are secure and diverse—facilitating greater domestic production, a range of supply, built-in redundancies, adequate stockpiles, safe and secure digital networks, and a world-class American manufacturing base and workforce."

As the following Executive order 14028 "Improving the Nation's Cybersecurity" (May 2021) directed; "Secretary of Commerce acting through the Director of NIST […] shall issue guidance identifying practices that enhance the security of the software supply chain." Such guidance shall include standards, procedures, or criteria" including [as extracted]: secure software development environments, maintain trusted source code in supply chains, employing automated tools to check for known and potential vulnerabilities, providing a purchaser a Software Bill of Materials (SBOM), and participating in vulnerability disclosure programs.

In 2022, the Industrial Control System Security firm Dragos noted in their annual report[5], "Cyber risk to the manufacturing sector is also increasing rapidly, led by disruptive cyberattacks impacting industrial processes, intrusions enabling information gathering and process information theft, and new activity from Industrial Control Systems (ICS)-targeting adversaries."

In their key findings, Dragos noted the following types of threat trends that have been observed specifically targeting the manufacturing sector:

- Ransomware with the ability to disrupt industrial processes is the biggest threat to manufacturing operations. Adversaries are increasingly adopting ICS-aware mechanisms within ransomware that could stop operations.

[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, and maintenance and other manuals

[5] Dragos *"2022 ICS/OT CYBERSECURITY YEAR IN REVIEW",* Copyright © 2022

- Disruptions within manufacturing industrial processes have supply chain implications that impact businesses and potentially operations elsewhere.
- The theft of proprietary and confidential manufacturing process details – often considered intellectual property – remains a high risk for manufacturers.
- A growing convergence of interconnected enterprise, operations, and process control networks contributes to a growing threat landscape.

Since then, the civil aviation sector and its suppliers have seen increased levels of ransomware and other attacks. These attempted attacks force many industry members to reevaluate their postures related to protecting our supply chain from ever increasing and relentless attacks.

To meet the need for a more resilient and secure supply chain, the civil aviation community is advocating specifically for changes to proposed regulations and industry standards to secure the supply chain for its manufacturing sector. The sector includes the organizations involved in designing and producing aircraft, maintenance, repair and overhaul of organizations, as well as the associated supply chain in supporting those organizations in their activities and supporting air and ground operations of aircraft. This will in turn provide benefit to the many operators and passengers who depend on the safety and security of our industry, and the products and services we provide every day.

1.2 Understanding the Complexity of the Civil Aviation Supply Chain

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 ecosystem encompasses 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 activities that impact the internal manufacture[6] 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.

This context gives rise to a matrix of issues, as shown in **Error! Reference source not found.**.

[6] 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

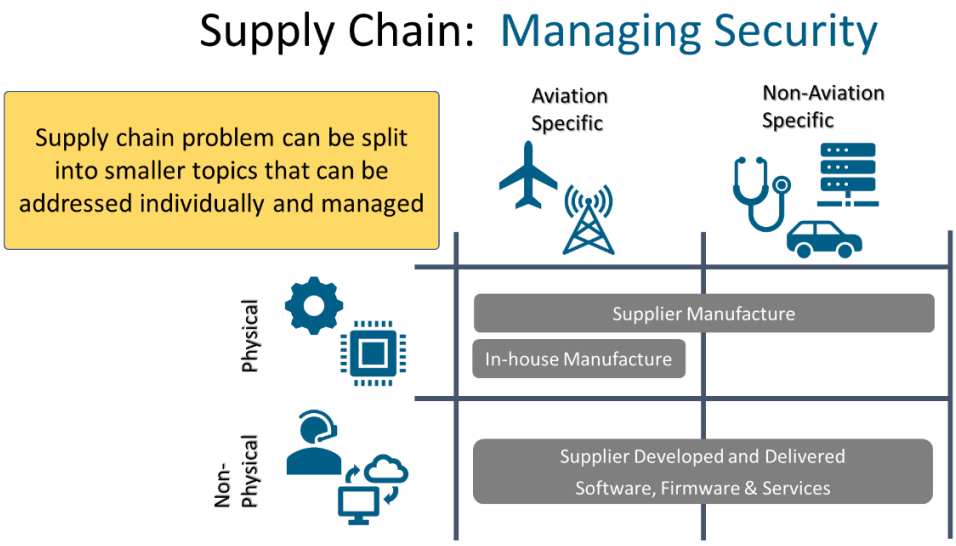

Figure 1: Supply Chain matrix

The diagram shows 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. Suppliers who mainly operate in other industry areas and are not subject to regulatory and/or commercial pressures to adopt aviation practices.

The products in the supply chain are split into physical items where the nature of cyberattacks are typically indirect – such as on the manufacturing equipment producing the physical items, or from cyberattacks to the systems used to design the items, or from the non-physical products (such as software) where cyberattacks may directly alter the product and its performance, as seen in the diagram.

1.3 Components of the Civil Aviation Supply Chain

The civil aviation supply chain extends far beyond even the baseline components of a given airplane or manufacturing line, and to be effective an industry view should therefore consider more than just the operational airplane products and systems, but instead include all systems that are used to support the products and operations. As core to aviation industry cyber safety and resilience, 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.

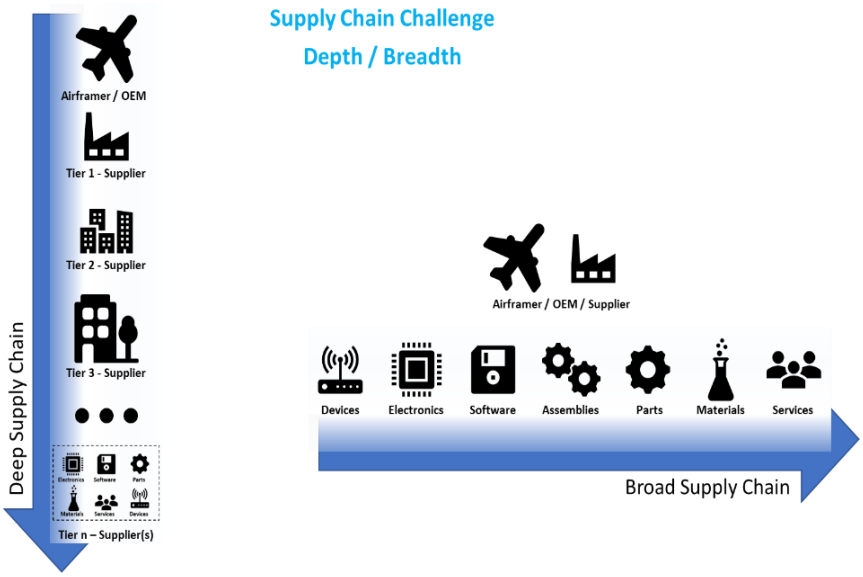

Figure 2: Illustration of vertical supply chain depth (left) for each OEM and horizontal supply chain breadth at each vertical level (right)

The threats posed to both vertical and horizontal supply chains 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.

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 could occur that would risk the safety and security resilience of civil aviation operations.

As such, systematic and proactive solutions to mitigate vulnerabilities associated to unaccepted risks must increase the resilience of individual systems as well as the entire ecosystem and provide multiple layers of defense. This will ensure 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.

1.4 AIA Civil Aviation Goals for Securing its 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 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 3 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.

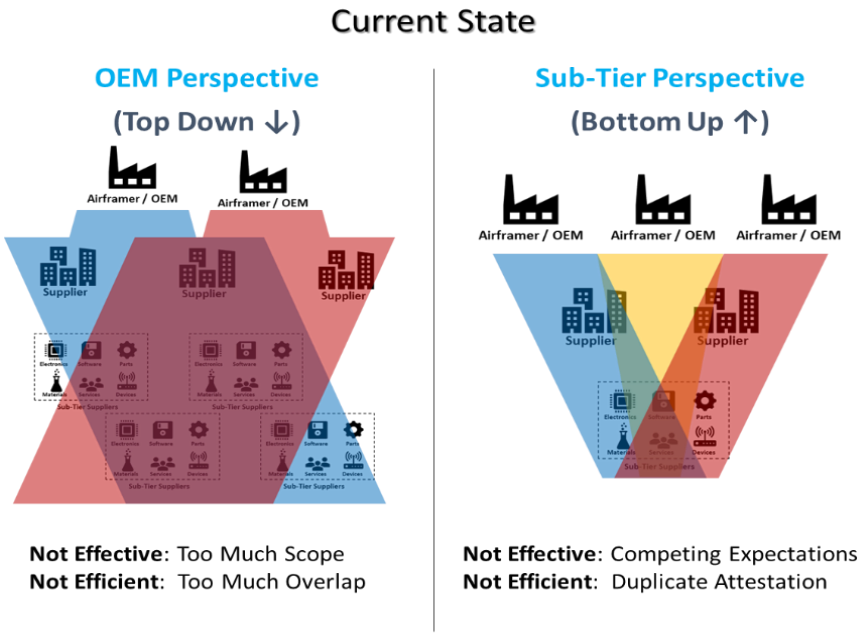

Figure 3: Current state (perspectives) for auditing and oversight of Cybersecurity Performance

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.

Error! Reference source not found. 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.

Proposed improvement scheme for auditing and oversight of Cybersecurity Performance

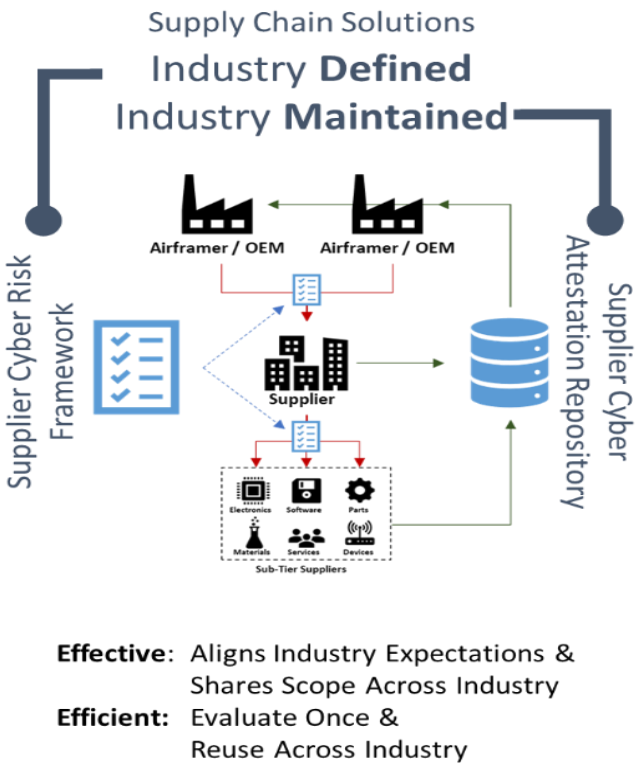

Figure 5: Proposed future auditing and oversight scheme for cybersecurity performance

For suppliers, this scheme would allow 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.

Within Europe, the European Cybersecurity for aviation Standards Coordination Group (ECSCG)[7] – which has been tasked with coordinating standards development. 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.

AIA has recommended that North America develop an equivalent body to the ECSCG and this has been established under US ACCESS (U.S. 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.

AIA also advocates to establish an Aviation Information Security Management System (ISMS) that would be analogous to the Safety Management System that is already mandated. The newly approved regulation (EU 2022/1645 and EU 2023/203) in Europe is termed Part IS. 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. While the regulation is focused on products and services that have a safety impact 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.

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

The formation of both US ACCESS and Aviation ISMS for aviation industry partners would encourage the development of common such as strategy, organization, and accountability within the North American aviation industry. In addition, the Aviation SMS would provide a consistent means for performing risk assessments of the organization and identifying threats with a common ranking of severity. This would in essence become a North American equivalent to the European Union's Part IS regulatory requirement.

1.5 Existing Regulations and Related Standards

Many nations have variations of Critical National Infrastructure regulations. The countries define which industries are considered 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 (NIS2) Directive[8].

In addition to these U.S. initiatives, EU Member States have additional Critical National Infrastructure regulations. The approaches between the U.S. and the EU differ as the manufacture of aerospace products and parts has been included in the critical manufacturing sector definition in the U.S. but the NIS2 Directive applies only to the operators of the infrastructure and manufacturers of aircraft components in a duplication of Part IS. 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 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.

1.6 Emerging Requirements and Standards for Civil Aviation's Supply Chain

With the advent of recent White House Executive Orders and the development this year (2023) of both a new National Cyber Strategy and National Cyber Strategy Implementation Plan, we expect to see significant and ongoing changes to the Civil Aviation Regulatory Requirements and Industry Standards that will likewise impact Civil Aviation throughout its Supply Chain.

Changes to U.S. Regulatory Requirements related to Supply Chain.

In early 2021, the Biden Administration generated two new Executive Orders related to enhancing Supply Chain Security

- Executive Order 14017 on "America's Supply Chains" (Feb 2021)
- Executive Order 14028 - "Improving the Nation's Cybersecurity" (May 2021)

In the second Executive Order related to "Improving the Nation's Cybersecurity", the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain.

Such guidance shall include standards, procedures, or criteria regarding [extracted]:

i. Secure software development environments
ii. Providing artifacts that demonstrate conformance.

[8] NIS2 Directive is published at European Union level in EU 2022/2555. As a Directive, this is transposed into national law for each Member State and specific regulation in each Member State needs to be observed.

iii. Employing automated tools, or comparable processes, to maintain trusted source code supply chains;
iv. Employing automated tools to check for known and potential vulnerabilities and remediate them;
v. Providing artifacts on completion of these actions;
vi. Maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services;
vii. Providing a purchaser a Software Bill of Materials (SBOM) for each product;
viii. Participating in a vulnerability disclosure program that includes a reporting and disclosure process;
ix. Attesting to conformity with secure software development practices; and
x. Ensuring the integrity and provenance of open source software used within any portion of a product.

2 Physical Goods and Software provided by Suppliers

While work is ongoing, the current minimum elements for Software Bill of Materials as defined by the Department of Commerce and other stakeholders, see link: "The Minimum Elements For a Software Bill of Materials (SBOM)", will require all Federal Organization to support basic SBOM functionality. AIA plans to release a follow-on white paper to recommend minimal elements and processes to be used in civil aviation adoption of SBOMs.

Outside of software, 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 normally manufactured by Suppliers in foundries under aerospace industry control.

AIA is providing a specific report on the use of Software Bill of Materials in the aviation sector.

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 Operational Technology from Supply Chain Partners

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, 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.

For structural components, the production of critical components and structures require cybersecurity risk monitoring. The regulations of Part 21[9] 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).

By adopting 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.

2.3 Securing Residual Risks from New and Legacy Operational Technologies

It will not be possible to secure all operational technologies (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. The inability to procure appropriate equipment or the use of legacy equipment especially 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 industry standards and guidance that should be considered include, NIST SP 800-161, NIST SP 800-82, the NIST Cybersecurity Framework for Manufacturing (NIST IR 8183), and the ISO 27000 family. NIST SP 800-82 that focuses on Industrial Control System Security 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.

NIST Special Publication 800-82, "Security Controls for Industrial Control Systems," 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.

Other industry standards such as 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.

AIA recommends establishing aviation specific standards for securing both enterprise and OT systems in a manner suitable for the aviation environment and the lifecycles that exist in aviation.

[9] 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 **Error! Reference source not found.**

These standards should form an Aviation Information Security Management System (akin to the European Union's Part IS program) that can be certified for simplified auditing and used as a means of compliance for any future regulations.

2.4 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.

2.5 Securing Design and Configuration Management of Complex Electronic Hardware (CEH)

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 (DO-178B/C / ED-12B/C), hardware (DO-254 / ED-80) and systems (SAE ARP 4754A / ED-79A). The SAE G-32 committee on Cyber-Physical 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 artifacts.

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 5.

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).

2.6 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 Data load Cyber Recommendations Report.

2.7 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 Cyber-Physical 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 reusing security components from other industries.

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 7 apply for the software development environment.

2.8 Delivery of Software

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 Data-load Cyber Recommendations Report.[10]

3 Non-Aviation Sector Manufacture of Physical Goods and Software

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

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

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 **Error! Reference source not found.** 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 are 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.

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 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.

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 here: 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.

3.3 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 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.

3.4 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 DO356A applies to inspections of non-aviation software.

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

3.5 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 include 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.

Among others, the Commonwealth Nations are now required to submit attestation documentation related to protecting against counterfeit components in their Information and Communications Technology systems, including that used to support Civil Aviation manufacturing and operations. Additionally, NIST 800-161 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) also provide aviation specific guidance for counterfeit policies. SAE AS 6174A provides additional guidance on detecting and avoiding counterfeit non-electronic material.

The DHS has provided guidance [11] on procurement 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.

Additionally, AIA recommends 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 RTCA DO-392/EUROCAE ED-206 and planned Revision A will provide guidance on vulnerability disclosure programs in an aviation environment.

4 Securing Manufacturing Sites with Supply Chain partners

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.

Suppliers must also be held accountable for the security of mobile devices and testing systems that are brought into manufacturing zones and operations.

[11] DHS Procurement Language Guidance; https://www.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf)

5 Vulnerability Management and Communications

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.

5.1 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.

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.

5.2 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.

A new publication provided by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, titled "A Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management" details a common framework and prescribed use cases that may be used to improve both visibility and responses to vulnerabilities in Supplier Hardware.

5.3 Vulnerability Communications

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 planned revision to RTCA - DO-392/EUROCAE – ED-206; "Guidance for Security Event Management" is expected to establish a new common scoring method and thresholds for civil aviation security event reporting, including for the aviation supply chain, to ensure consistency across aviation in reporting and resolving vulnerabilities.

6 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.

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 confidence in suppliers by repeated randomized testing. It may therefore be ultimately cheaper to establish trust in such suppliers, rather 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. AIA has already established its position related to Cybersecurity Testing for the Civil Aviation sector in its White Paper published in 2020.

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 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.

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

The RTCA DO391 / EUROCAE ED-201A "Aeronautical Information System Security Framework Guidance" standard provides 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.

6.1 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.

6.2 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.

7 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.

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.

8 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. It has been noted that no specific recommendations are made at this time other than to establish trust and extend existing standards with cyber for penetration into non-aviation markets.

9 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.

As further guidance to assist organizations in procuring cloud services, NIST published **Special Publication (SP) 800-210,** General Access Control Guidance for Cloud Systems, which presents an initial step toward understanding security challenges in cloud systems by analyzing the access control (AC) considerations in all three cloud service delivery models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Essential characteristics that would affect the Cloud's AC design are also summarized, such as broad network access, resource pooling, rapid elasticity, measured service, and data sharing.

10 Next Steps

AIA recommends the Civil Aviation industry move forward rapidly to revise its industry standards related to Supply Chain cybersecurity performance, while also helping Suppliers improve their cybersecurity postures and vulnerability management programs.

The recommendations contained within this report have been summarized for clarity and identifying the continuing efforts to put these recommendations in practice. Table 1 lists the major recommendations for further industry reports and standardization activities.

Table 1 Recommendation of further recommendation reports and standards

Recommendations	**Target group**	**Target Standard**
Establish trust framework for aviation cybersecurity covering: - Aviation and non-aviation supply chain - IT and OT interface	AIA / ASD ISO / IEC / IECQ	New standard

Recommendations	**Target group**	**Target Standard**
Establish cybersecurity certification auditing guidelines on: - DO-326A/DO-356A (ED-202A/ED-203A) - Component validation	AIA/ASD	Updates to DO-326A/ED-202A & DO-356A/ED-203A,
Develop guidance on aviation component vulnerability subjects: - Common scoring and communications - Legacy protocol/software accountability	RTCA SC-216 EUROCAE WG-72	DO-392/ED-206
Develop a Software Bill of Materials standard or format for civil aviation	AIA, RTCA SC-216, EUROCAE WG-72, IAQG	Requires updates to multiple industry standards
Develop a report for securing cloud services used in aviation	AIA	New Report

11 Conclusions

In building this report, AIA has only begun to consider the incredible task at hand in attempting to develop adequate cybersecurity and resilience to even partially address the growing enormity and complexity of our Civil Aviation Supply Chain.

While the extent and complexity alone of the Civil Aviation Supply Chain is so daunting to be nearly impossible to address, the new reality of facing much increased threats and precisely targeted attacks across our supply chain affects all of us, This severely threatens the safety and security of our industry going forward, and leads us to believe that a single solution cannot address all these concerns nor offer the ability to harmonize across all the regulatory guidance and industry standards needed to address the breadth and depth of our supply chain.

As such, AIA is calling for a series of urgent and focused government and industry actions, aimed at developing a new strategy to focus regulatory guidance/actions and new industry standards to secure our supply chain, and at many levels and functions (e.g. design, build, operate). This will enable us to begin to move holistically to harmonize all of the interwoven regulatory, industry standard, and contractual actions needed to improve the security and resilience of the aviation supply chain.

The actions should begin with developing new standards and regulations that are specific to aviation, versus those that do not follow aviation regulations and practices, as well as better defining the software/hardware bill of material level information to better identify potential weaknesses in our systems and move to address these with both corrective and preventative actions. In doing so, the strategy must continuously identify areas for future development and improvement, including improvements to the specifications used for the procurement of general services, and the need for new strategies to address the appropriate use and security of cloud services and data retention used for aviation.

Finally, AIA acknowledges the real strength of Civil Aviation has always been the close cooperation between government, industry, and its industry standards organizations to remain focused on the safety and resiliency of our industry. It is this strength that we will draw on now to address the security and resilience of our industry critical supply chain and all its functions.

12 Appendices

12.1 Summary of Civil Aviation Supply Chain-related Quality and Safety Regulations

Source	Title	Subject Matter
14 CFR Part 21.137[12]	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[13] 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.
Add Part 25		
21.A.124[14]	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.*
21.A.139[15]	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[16]	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. EIA-STD-4899 provides industry standard for preparing plan.

[12] As current in e-CFR as of May 7, 2020 equivalent to Amendment 21-100
[13] Ibid.
[14] As current in EU 748/2012
[15] Ibid.
[16] 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 8120.12A	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.
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.

A number of standards exist or are in work that support the supply chain efforts and are listed in the following **Error! Reference source not found.**:

Table 2 Standards supporting supply chain efforts

Identifier	Title	Subject Matter
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
IEC 62668-2	Managing electronic components from non-franchised sources	Provides extension to IEC TS 62668-1 on sourcing components from non-franchised distributors.

Identifier	Title	Subject Matter
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
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

Identifier	Title	Subject Matter
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 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.
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 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 12.3 lists all references quoted in this document including the latest known revisions at time of publication of this document for information.

12.2 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

12.3 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	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 Delegated Regulation (EU) 2022/1645 *(Part IS)*	Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014
Commission Implementing Regulation (EU) 2023/203 *(Part IS)*	Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664
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

Reference	Title
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
Directive (EU) 2022/2555 *(NIS2 Directive)*	Directive (EU) 2022/2555 Of The European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
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-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

Reference	Title
EUROCAE ED-201A *(equivalent to RTCA DO-391)*	Aeronautical Information System Security Framework Guidance
EUROCAE ED-206 *(equivalent to RTCA DO-392)*	Guidance on Security Event Management
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
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
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

Reference	Title
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
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

Reference	Title
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-391 *(equivalent to EUROCAE ED-201A)*	Aeronautical Information System Security Framework Guidance
RTCA DO-392 *(equivalent to EUROCAE ED-206)*	Guidance on Security Event Management
SAE ARP 4754A *(equivalent to EUROCAE ED-79A)*	Guidelines for Development of Civil Aircraft and Systems
SAE AS 5553C	Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition
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 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