



Aerospace Industries Association

Civil Aviation Cybersecurity Subcommittee Cybersecurity Testing Recommendations

Civil Aviation Cybersecurity Subcommittee & Advisory Working Group Members

Hank Wynsma – Chair, AIA Civil Aviation Cybersecurity
Subcommittee, General Electric Aviation

Sean Sullivan - Vice Chair, Civil Aviation Cybersecurity
Subcommittee, Boeing Commercial Airplanes

Working Group Members

Will Gonzalez	FAA
Varun Khanna	FAA
MW Davis	FAA
Cyrille Rosay	EASA
Jeff Troy	Aviation ISAC, GE
Xavier Depin	Airbus
Alain Combes	Airbus
Kanwal Reen	Collins Aerospace
Ted Kalthoff	Bombardier
Poliana de Moraes	Embraer
Stephen Porter	BAE Systems
Ruchik Amin	GE Aviation
Aaron Renshaw	American Airlines
Todd Trncak	American Airlines
Patrick McTernen	American Airlines
Casey Theisen	United Airlines
Becky Selzer	United Airlines
Fabian Lamba	Lufthansa Group
Frank Hundrieser	Lufthansa Group
Krzysztof Marek Milczewski	Lufthansa Group
Bill Bryant	MTSI
Sam Singer	Boeing, Senior Counsel (Cybersecurity)
Caroline Prado	Boeing
Brad Metrolis	Boeing
Tom McGoogan	Boeing (White Paper Focal)

Summary

AIA acknowledges civil aviation industry partners, including regulators, airplane manufacturers, airline operators, component suppliers, and those building and operating the infrastructure of the global aviation industry all have a common goal – safety.

As cybersecurity risk in the aviation industry continues to expand and evolve, aviation industry businesses and organizations are seeking methods to provide continuous assurance, that the digital components of aircraft and supporting aviation infrastructure are safe and uncompromised.

This AIA paper considers the importance of both safety and cybersecurity objectives for aviation industry stakeholders along with the risks that may result from testing certified aircraft, ground systems, and its associated equipment.

This paper is intended to clarify AIA's position related to the roles, responsibilities, and obligations of Regulators, Operators, OEMs, and Suppliers for airplane or other system testing. This includes testing and technical evaluations that could potentially impact the integrity and safety of airplanes and ground support services.

Executive Summary

Airplane manufacturers, airline/cargo operators, component suppliers, regulators, and those building and operating the infrastructure of the global aviation industry all have a common goal – SAFETY.

As cybersecurity risk in the aviation industry continues to expand and evolve. Many aviation industry businesses and organizations are seeking methods to provide continuous assurance and validation, that the digital components of aircraft and supporting aviation infrastructure remain safe and uncompromised.

AIA recognizes the evolving risks to digital components, the safety objectives of all industry stakeholders and the risks that may occur in testing previously certified airplanes and ground support equipment. Additionally, new cybersecurity risks may emerge after type certification that must be continuously reviewed and verified in terms of potential airplane and ground system impacts.

AIA is also aware a growing number of operators have begun to pursue options to conduct their own technical risk assessments and testing or develop other means to understand risks that may emerge post type certification, either as newly identified vulnerabilities or through modifications or other configuration changes requiring Supplement Type Certification or other re-validation of the safety and security of the airplane and its components.

AIA concurs with FAA, GAO, and industry standards stating concerns that cybersecurity testing of operational aircraft may have potentially severe consequences resulting in regulatory non-compliance and potentially creating a safety event.

As such, AIA considers direct testing of operational aircraft should remain the very last alternative method to address cybersecurity risks. This includes reducing the potential for cybersecurity testing and other technical evaluation to negatively impact the integrity and safety of our civil aviation industry, including its airplanes and ground support services.

Instead, AIA recommends aircraft manufacturers, component suppliers, and airline operators partner together on the development of methods and procedures are conducted in protected laboratory or other controlled environments with measures in place to ensure these activities cause no operational reliability concerns or additional safety risks to global air travel.

Contents

1	Civil Aviation Cybersecurity Testing Overview	6
1.1	Background	6
1.2	Purpose	7
1.3	Applicable Requirements	7
1.3.1	Federal Aviation Administration (FAA) Security Requirements	8
1.3.1.1	Other International Regulatory Requirements and Guidance	8
2	Proposed Guidance	9
3	Stakeholder Roles and Responsibilities	10
2.1	Operator Responsibilities	10
3.1	OEM and Component Supplier Responsibilities	11
4	Stakeholder Recommendations	11
4.1	Operator Recommendations	11
4.2	OEM and Component Supplier Recommendations	12
4.3	Regulator Recommendations	13
5	Information Protections related to Cybersecurity Testing	14
5.1	FAA and TSA Sensitive Security Information Management Requirements	14
5.2	Information Protections and Sharing Restrictions	14
6	Overarching Recommendations for Civil Aviation	15
7	Existing regulations and related standards	17
8	Abbreviations	19
9	List of References	21

Tables

Table 1	Existing civil aviation quality and safety regulations for supply chain	7
Table 2	Standards supporting airplane testing requirements	9
Table 3	Proposal for Security Level assignment in Operational Technology used to produce structural items	12
Table 4	Proposal for Security Level assignment in Operational Technology used to produce electronic components and assemblies	12
Table 5	Recommendation of further recommendation reports and standards	18

1 Civil Aviation Cybersecurity Testing Overview

In the world of cyber security, there is a requirement for system operators to continuously search for vulnerabilities. This AIA position paper seeks to inform aviation industry partners on the risks that are associated with cybersecurity testing, while also identifying appropriate roles and recommendations for Regulators, Operators, OEMs, and Component Suppliers as they turn to face these challenges going forward.

Performing testing and technical evaluations of aircraft system and components are highly complex, and even more so when it comes to the details needed to set up and conduct cybersecurity-specific evaluations. This is further complicated by the many overlapping roles among aviation industry partners related to technical evaluation of aircraft and its supporting ground systems that are needed to meet the immutable safety and security requirements of civil aviation.

As Operators and other industry stakeholders all have a role in assessing and controlling aviation cybersecurity risks to the global aviation ecosystem, it remains critically important and essential that Regulators, Operators, OEMs, and Component Suppliers all work together to avoid any action that could impact aircraft safety and security, including aircraft and ground system conformity that could affect aircraft and component type certifications for airworthiness.

1.1 Background

The aviation industry continuously faces a multitude of cybersecurity risks. While airplane system and network designs for safety and airworthiness have served to protect the industry from many of these risks, we understand we must constantly evaluate new risks and seek reassurance our aircraft designs and in-service operations remain resilient. Many aviation industry businesses and organizations are seeking methods to provide assurance the digital components of aircraft and supporting aviation infrastructure are safe and have not been compromised.

In an October 2020 report on Aviation Cyber Security¹ the GAO recommended the aviation industry conduct periodic independent testing of aircraft. In the report, GAO also stated “Both airlines and airframe manufacturers expressed concerns that penetration testing could negatively affect an airplane’s network and systems configurations. Further, misconfigurations that could affect an airplane’s airworthiness might not become apparent until an airplane is put back into service and a problem occurs.

However, it is notable the FAA decided not to concur with this testing recommendation. In its published comments about the report, the FAA stated “The FAA believes any type of testing conducted on the in-service fleet could result in potential corruption of airplane systems, jeopardizing safety rather than detecting cybersecurity safety issues. Should a cybersecurity safety issue occur, the FAA has processes in place to address and correct the safety issue.”

Additionally, DO-355A also states that “invasive testing such as that requiring code injection or system tampering on a certified and conformed, delivered airplane risks the airplanes Airworthiness Certification. This could result in non-conformance to the type design of the airplane and lead to airplane grounding.”

¹ GAO-21-86, <https://www.gao.gov/products/gao-21-86>
Civil Aviation Cybersecurity Subcommittee Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928 | 703.358.1000 | www.aia-aerospace.org

It is critical for the aviation industry to fully understand the implications of conducting cybersecurity testing and technical evaluations of an aircraft: as these efforts are highly complex requiring deep knowledge of airplane connectivity and systems engineering. Even a simple change must be considered for its impact to conformity and prior aircraft type certifications for safety and airworthiness.

Recognizing the desire of the industry to obtain continuous assurance of the cybersecurity state of aircraft, this paper opines that all aviation stakeholders must carefully consider the implications of cybersecurity testing on physical aircraft and supporting systems.

1.2 Purpose

In considering the increased interest in cybersecurity testing, AIA is committed to ensuring commercial aviation remains both safe and secure, meeting or exceeding all applicable regulatory requirements for both physical and cybersecurity.

As such, this paper is intended to:

1. Develop a common harmonized understanding of Regulator, OEM, Operator, and Component Supplier in achieving cybersecurity objectives for the civil aviation industry.
2. Carefully consider the need for the aviation industry partners to face together the ever evolving nature of cybersecurity risks to aviation.
3. Acknowledge the potential for airworthiness and type conformity consequences from cybersecurity testing on actual aircraft [per DO-355A] and encourages the aviation industry to focus on detailed technical evaluations, making use of off airplane lab and network testing wherever possible.
4. Set clear objectives and delineate between requirements for tests and technical evaluations that are completed by OEMs and Suppliers on a recurring basis as part of the overall aircraft/system certification process, against those required by Operators to meet their own risk assessments and regulatory assurance requirements.
5. Identify overlapping boundaries of security responsibilities [and regulatory requirements] shared by Regulators, Operators, OEMs and Component Suppliers.
6. Reaffirms the roles Regulators, Operators, OEMs, and Component Suppliers, all play in maintaining continued airworthiness, in regards to cyber security.

1.3 Applicable Requirements

In considering cybersecurity testing and other technical evaluation activities to address applicable requirements, Operators must understand potential airworthiness and type conformity consequences that may occur as a result of such testing and technical evaluations.

14 CFR Part 121.703 – Service Difficulty Reports, lists requirements for Operators to report to Airlines and Authorities items related to in service issues. Additionally, AC 119-1: Regulations (14 CFR) parts 121, 121/135, 125, and 129, stipulate that operators must develop and maintain FAA-authorized Aircraft Network Security Programs (ANSP) that are sufficiently comprehensive in scope and detail to accomplish risk assessments under the following four use cases to address OpsSpec D301 requirements as derived from DO-355 and DO-355A as industry standards.

However, as noted in Appendix B, page B-6 of DO-355A the following statement addresses invasive testing relating to cybersecurity:

“Airplane Testing Disclaimer: Invasive testing such as that requiring code injection or system tampering on a certified and conformed, delivered airplane risks the airplane’s Airworthiness Certification. This could result in non-conformance to the type design of the airplane and lead to airplane grounding.”

Additionally, DO-355A states in section 10.3 that “The DAH should provide the information security assumptions that have been used within a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance to the operator.”

As such, while applicability of the requirements is noted to include requirements for both Operators and OEMs to review their security assumptions and assessments of risks as noted in DO-326A, DO-355A, and DO-356A, these industry standards do not automatically indicate a need for cybersecurity testing, which could lead either intentionally or unintentionally to potential non-conformance with airworthiness certification.

1.3.1 Federal Aviation Administration (FAA) Security Requirements

The following provides a regulatory basis for FAA Design Holder and Operators for meeting and maintaining type certification of aircraft and to ensure safety and airworthiness for aircraft in both ground and flight operations.

14 CFR Part 25 – AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES

14 CFR Part 21.3 – FAA Design Holder Reporting Requirements, “Reporting of failures, malfunctions, and defects.”

14 CFR Part 121 703 – Service Difficulty Reports, lists requirements for Operators to Report to Airlines and Authorities related to service issues.

14 CFR Part 21.137 – FAA Design Holder Reporting Requirements, “Quality System”

49 CFR Parts 15 and 15.20 – Sensitive Security Information (SSI) for restriction of information.

FAA Order 1600.75 – Protecting Sensitive Unclassified Information (SUI) [Restricted Document]

AC 43-216; “Software Management During Aircraft Maintenance”

AC 119-1 – Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP)

AC 20-152A/ AMC 20-152A – Development Assurance for Airborne Electronic Hardware

1.3.1.1 Other International Regulatory Requirements and Guidance

In addition to existing Federal Aviation Administration (FAA) and Transportation Safety Administration (TSA) regulations, many other international aviation industry regulatory authorities expect international operators to follow regulatory requirements and guidance related to specific data security, data rights, testing, and other verification of compliance that are unique to national and international operating requirements and applicable regulations.

Within the European Union, the European Union Aviation Safety Agency (EASA) provides guidance and specifications as Instructions for Continuing Airworthiness, including;

EASA AMC 20-42 - General Acceptable Means of Compliance for Airworthiness of Products, Parts, and Appliances provides European Union Aviation Safety Agency (EASA) Guidance for Airworthiness Information Security Risk Assessments

EASA Certification Specification CS-25, Subpart F – Equipment (CS 25.1319) requires aeroplane equipment, systems and networks be protected from intentional unauthorized electronic interactions (IUEA) that may result in adverse effects to the safety of the aeroplane.

2 Proposed Guidance

For policies relating to cybersecurity testing, operators should consider what has already been tested for type certification and the potential for additional consequences that could occur from independent testing.

AIA's position and guidance regarding airplane and certified ground support systems as it relates to cybersecurity testing and technical evaluations is stated as follows:

1. As direct testing of operational aircraft carries the potential for additional significant risks, AIA recommends industry partners carefully consider these risks, and work together to put in perspective of the objective sought and justified through risk analysis to reassure industry stakeholders of the continued airworthiness and resilience of the aircraft tested.
2. AIA recommends aviation industry stakeholders work together to consider cybersecurity risks or threats may emerge after type certification or may need to be reconsidered and verified as a result of modification or other changes as part of supplemental type certification.
3. AIA recognizes OEMs and Component Suppliers are required per Part 25, Part 21, and Part 33 regulations to ensure safety and airworthiness of aircraft and supporting systems, taking into account industry standards used throughout the aviation industry. This is accomplished through detailed risk analyses, flow down of requirements, and multiple levels of technical evaluations and testing.
4. AIA understands Operators primarily focus their risk assessments on requirements for validation and implementation of ANSPs, as stated in AC 119-1, or any additional operational considerations and regulatory compliance requirements placed on operators. As such, it is expected that Operators will continue to seek additional information on prior risk assessments and technical evaluations performed by OEMs and Component Suppliers for regulatory approval & review also to support their ANSPs.
5. When an Operator or Maintenance, Repair or Overhaul (MRO) organization performs post-production modifications to an airplane (Supplemental Type Certification), OEMs and Component Supplier should be prepared to provide additional subject matter expertise and other advisory support to assist the operators in maintaining airplane type conformity and airworthiness.
6. To support testing and technical evaluation activities, Operators, OEMs, and other stakeholders should identify a select set of trusted individuals who are allowed access to more testing and configuration details.

7. If independent testing organizations are used, it is important all parties sign appropriate non-disclosure agreements and other legal obligations to protect any intellectual property and other sensitive information that may be associated with the testing activities.
8. AIA members must finally ensure all materials related to their own or 3rd party technical evaluations and testing are secured and protected in accordance with all applicable contractual and legal considerations (e.g., ITAR, SSI, intellectual property (IP) restrictions and obligations).

3 Stakeholder Roles and Responsibilities

AIA acknowledges that Operators, OEMs, Component Suppliers will all need to periodically demonstrate to both their own leadership and various international regulators that they are adequately considering risks to airplanes in operations, as well as the security and risk management of ground support and maintenance systems.

The following details some of the stakeholder roles and responsibilities to be supported in this context.

2.1 Operator Responsibilities

Operators are responsible to develop and validate their own Airplane Network Security Plans, per AC 119-1- Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP) to maintain continued airworthiness for their type certified aircraft.

While Operators are not directly responsible for all aspects of cybersecurity relating to airplane hardware and software, they are required to adhere to Instructions for Continuing Airworthiness (ICA). As identified in Operator ANSPs, Operators assume responsibilities for ensuring adequate protections for the airplanes as configured and certified when in maintenance or in service.

Per AC 119-1: Regulations (14 CFR) parts 121, 121/135, 125, and 129, operators must develop and maintain FAA-authorized Aircraft Network Security Programs (ANSP) that are sufficiently comprehensive in scope and detail to accomplish the following four items:

1. Ensure data security protections are sufficient to prevent access by unauthorized devices or personnel external to the aircraft.
2. Ensure security threats specific to the certificate holder's operations are identified and assessed, and that risk mitigation strategies are implemented to ensure the continued airworthiness of the aircraft.
3. Prevent inadvertent or malicious changes to the aircraft network, including those possibly caused by maintenance activity.
4. Prevent unauthorized access from sources onboard the aircraft.

AC 119-1 (as derived from FAA OpsSpec D301) for airplane airworthiness and regulatory compliance also notes the following Operator-level responsibilities:

- Operators retain responsibility to comply with guidance for security configuration management and access control for all ground systems that connect to its airplanes.

- Operator use of 3rd party connectivity and services are the responsibility of the Operator to ensure they are compliant with regulatory requirements.

3.1 OEM and Component Supplier Responsibilities

For Aviation Industry OEMs and Component Suppliers, the 14 Code of Federal Regulations for Part 21, Part 25 and Part 33 systems consider primary and secondary structures.

Additionally, AC 20-152A / AMC 20-152A – Development Assurance for Airborne Electronic Hardware considers complex electronic hardware installed in an aircraft may have multiple electronic interactions and thus the design needs to specifically consider security.

RTCA DO-356A (ED-203A) also sets forth guidance to ensure security in the design 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).

As such, OEMs and Component Suppliers utilize a three-tier approach to certify aircraft where primary and secondary structures are considered for the potential for failures that could have a direct Catastrophic or Hazardous effect have a Hazardous or Major effect, while other structures and systems are considered Non-Essential Equipment and Furnishings (NEF), having only a marginal potential impact to safety and airworthiness for design assurance.

The standards for software in DO-356A / ED-203A also set the objectives for the design of products. For software design, 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. SAE AS 91115 does establish quality standards for the security of aviation industry software development environments that may be used by software security auditors.

It is the obligation of OEMs and Component Suppliers to provide to the Operator in-service security processes to maintain the security level of the aircraft and to support operational risk assessments, including in-service security updates through service bulletin or airworthiness directives.

4 Stakeholder Recommendations

4.1 Operator Recommendations

For airplane security testing related to embedded airplane systems and networks, AIA provides the following recommendations:

- 1) Operators should contact their OEMs and hardware vendors prior to attempting their own risk assessments involving either airplane equipment or components. OEMs and system providers with Design Assurance Holder responsibilities may then provide information related to previously completed cybersecurity technical evaluations, and

provide guidance related to maintaining type design conformity and other airplane configuration risks that could occur as a result of cybersecurity testing activities.

- 2) Operators should not take any action that changes hardware, firmware or software configurations on the aircraft, including invasive testing, modifications to aircraft hardware, configuration modules and changing loadable software. Doing so could result in the operator losing airplane airworthiness and type design conformity, with the potential consequence of aircraft grounding.
- 3) Operators' concerns over emerging vulnerabilities or new threats potentially impacting the product overall should be collected, consolidated, and shared with their OEM and Component Supplier partners for civil aviation industry awareness and follow up action if applicable.
- 4) All operator personnel involved in testing and technical evaluation activities should review standards associated with Aircraft Security Operator Guidance (ASOG) per DO326A, and attend if needed any relevant training offered by the Design Holder(s) in order to become more familiar with specific airplane architecture and regulatory requirements.
- 5) Operators must strictly control any equipment used to perform testing, so that all data that may be accessed and/or ex-filtrated after testing will remain under strict control. Testing equipment and post testing documentation will likely include technical information on proprietary interfaces and other Intellectual Property (IP).
- 6) In the event Operators utilize subcontractors, they must sanitize all data and test results from other suppliers or end systems between dissimilar parties. Aviation Industry Partners must ensure that adequate non-disclosure and other information handling agreements are in place so they do not improperly distribute or store proprietary or security sensitive data resulting from testing.”
- 7) Operators should finally ensure all test data and documentation which contains details of airplane architecture, potential security weaknesses, system configurations or security test material including Intellectual Property (IP) should be classified and treated accordingly in correspondence with all regulatory and contractual requirements.

4.2 OEM and Component Supplier Recommendations

All stakeholders in the aviation eco-system are responsible for securing the systems they operate to include assurance of safety and security of sub-systems. Regardless of the capability of a supplier, aviation industry companies must verify the cyber secure state of equipment that is operated and relied upon then trust it for operations.

AIA provides the following recommendations to its OEMs and Component Suppliers:

- 1) OEMs and Suppliers should proactively work with Operators to determine scoping requirements for testing aircraft and component systems to include previous test results.
- 2) OEMs and Component Suppliers must be prepared to support Operator requests and assist in the review of their airplane testing objectives and develop and configure facilities and other means to support supplemental type certification requirements.

- 3) OEMs and Component Suppliers should be prepared to support additional Operator requests for low level risk and technical assessments needed to support airline/cargo carrier operations and information needed for their ANSP activities.
- 4) For new technologies and solutions, the OEMs should provide the option for customers (airlines) to test their respective solutions on a test bench before incorporating them into/onto the actual aircraft.
- 5) OEMs should develop a framework similar to Common Vulnerability and Exposure(s) (CVEs) used by many organizations today for enterprise level vulnerabilities, but specialized to relate more appropriately to the physical and product security protections used for aircraft-specific systems and networks. Also a Common Vulnerability Scoring System (CVSS)-like scoring system should be specific to e-Enabled Aircraft and access controls in terms of compute and help prioritize related risks.
- 6) OEMs and Component Suppliers should address any action that changes any hardware, firmware or software configurations on the aircraft has been verified for safety and airworthiness.
- 7) OEMs must ensure any actions to be taken by Operators related to verification of safety and airworthiness are adequately covered in Service Bulletins and maintenance documentation.
- 8) OEMs should ensure all appropriate legal and contractual agreements should be written to allow all stakeholders to be given access to the appropriate level of technical information. In accordance with the concept of “need to know,” OEMs may also seek to limit the number of stakeholder personnel with access to sensitive cybersecurity testing information and results.
- 9) OEMs and Component Suppliers should be prepared to provide information related to similar testing, and provide guidance related to maintaining type design conformity and airplane configuration requirements that may be impacted by testing activities.
- 10) OEMs and Component Suppliers must ensure that all test data that includes airplane architecture, potential security weaknesses, system configurations or security testing are properly classified in correspondence with all regulatory and contractual constraints.

4.3 Regulator Recommendations

- 1) Recommend Regulator(s) review existing regulatory requirements and guidance to specifically address cybersecurity testing in terms of industry objectives and approve processes, procedures, and restrictions.
- 2) Recommends Regulator(s) to define the process for sharing to safely and securely disclose vulnerability and threat information safely and securely among between OEMs, Operators, and per ISEM DO-392/ED-206.
- 3) Recommends Regulator(s) provide means for continuing to validate ICA compliance under D301 for cyber security evaluations and testing to be conducted as attacker capabilities evolve.

- 4) Recommend Regulator (s) work with OEMs, Operators, and Suppliers to establish processes for addressing and correcting identified cyber safety issues. (as mentioned above)

5 Information Protections related to Cybersecurity Testing

5.1 FAA and TSA Sensitive Security Information Management Requirements

Commercial Aviation (including both Airplanes and Ground Support) 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). DO-326A/ED-202A, DO-355A/ED-204A, and DO-356A/ED-203A, also set industry standards for aviation parts and products to have the necessary framework so they may be appropriately secured.

Commercial Airplane platforms are therefore categorized by the U.S. government as critical transportation infrastructure, industrial controls systems, and critical manufacturing, and airplane information that, if publicly released would be detrimental to transportation security, is therefore subject to information protection requirements as "Sensitive Security Information" (SSI) as defined and regulated by the Department of Homeland Security.

AIA strongly advises anyone involved in cybersecurity testing and technical evaluations be fully informed and trained to the processes established in 49 CFR Parts 15 and 15.20 – Sensitive Security Information (SSI) for restriction of information, and if necessary for their roles, also FAA Order 1600.75 – Protecting Sensitive Unclassified Information (SUI) [Restricted Document].


AIA also acknowledges there may be other international regulatory requirements that relate to the protection of sensitive security information that must be followed if applicable to the operator(s).




5.2 Information Protections and Sharing Restrictions

All materials related to the testing must be properly secured and controlled, lest information relating to the test procedure itself may divulge sensitive and/or proprietary information relating to airplane configurations or give attackers a public playbook of what has been tested and where testing has not been performed and an exploitable vulnerability may be found.

AIA recommends civil aviation partners make use of Department of Homeland Security's Traffic Light Protocol (TLP) (see link: <https://www.cisa.gov/tlp>) or other information sharing agreements and/or controls as a means to ensure that cybersecurity testing sensitive information is shared only with appropriate parties associated with the testing, and protected from open distribution.

The following table describes the types of information sharing restrictions that may be established for both sources of cybersecurity testing information and recipients of that information as prescribed under the Traffic Light Protocol method.

TLP Protocol	When to utilize protocol	Sharing requirements
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>

<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing, and these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>

Commercial Airplane Operators and Field Service Bases are reminded per FAA Order 1600.75 Protecting Sensitive Unclassified Information (SUI), any documentation that may include sensitive data related to testing results or other technical evaluation details that result from testing, that the following language should be used in the footer of the documentation:

"Warning; This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520."

6 Overarching Recommendations for Civil Aviation

In considering its position relating to cybersecurity testing, AIA remains focused on ensuring the safety and airworthiness of the civil aviation industry and the flying public remains paramount to any other concern. The overarching recommendations reflecting the AIA Cybersecurity Testing position for Civil Aviation are summarized as follows.

Before proceeding with airplane cybersecurity testing, aviation industry stakeholders should consider:

- 1) In lieu of direct testing of operational aircraft, aircraft manufacturers, component suppliers, and airline operators should partner on the development of methods and capabilities to support cybersecurity technical evaluations and testing to be conducted instead in properly configured laboratories or other controlled environments to reduce residual risks to operational aircraft networks and systems.
- 2) Work together to clarify whether any proposed Cybersecurity Testing objectives are within valid scope for Aviation Industry OEMs and Component Suppliers (Part 21, Part 25, Part 33), or appropriately considered under Part 121 responsibilities for Operators.
- 3) Aviation industry stakeholders should consider sharing security concerns not just on an individual basis, but rather contribute to a set of commonly agreed sorting of cyber risks to be shared also with Operators, OEMs, System suppliers and Regulators, also to make better use of limited technical evaluation and testing resources.
- 4) Determine if any cybersecurity concerns in question may have already been addressed in other technical evaluation/testing activities, and to seek guidance related to maintaining type design conformity.

- 5) Ensure all applicable regulatory requirements and industry standards for cybersecurity testing are considered by all participants, especially for any testing involving aircraft overall design including complex electronic hardware.
- 6) Advocate for developing new guidance or updates to existing guidance and industry standards relating to cybersecurity technical evaluations and testing that are not covered in existing governance.
- 7) Provide means to ensure any findings and lessons learned from cybersecurity technical evaluations and testing are shared and distributed to all affected industry partners for follow on review and action.

Table 5 Recommendations for Participating Organizations and Relevant Standards

Recommendation(s)	Organization	Relevant Standards
Update AC119-1 and other FAA advisory publications to specify OEM, Operator, and Component Supplier responsibilities relating to cybersecurity testing	FAA	DO-355A
Determine whether proposed testing objectives may be accomplished in whole or part using existing laboratory equipment and networks	FAA, OEMs, Operators, Component Suppliers	DO-355A
Specify suggested parameters and release approval process to allow Operators to review testing results and risk assessments from prior aircraft cybersecurity testing conducted by OEMs and Component Suppliers	FAA (with inputs from OEMs, Operators, and Component Suppliers)	DO-326A, DO-355A, DO-356A
Ensure any personnel or subcontractors involved in airplane and ground testing and technical evaluation activities are fully trained on airplane architecture and regulatory requirements.	FAA, OEMs, Operators, Component Suppliers	DO-356A, DO-355A
Update security classification and handling requirements for data associated with aircraft cybersecurity testing.	FAA, TSA (with inputs from OEMs, Operators, and Component Suppliers)	49 CFR Parts 15 and 1520

7 Existing regulations and related standards

Table 1 Existing civil aviation quality and safety regulations

Source	Title	Subject Matter
14 CFR Part 21.137 ²	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 ³ 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.139 ⁴	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. <i>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</i>
<u>AC43-216</u>	<u>Software Management During Aircraft Maintenance</u>	Details processes to manage and secure SW used in maintenance
AC119--1	Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP)	Requires operators to validate security controls to ensure safety and airworthiness of aircraft remain in type certified conditions.
AC20-152A / AMC20-152A ⁵	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.
ED Decision 2020/006/R	Executive Director Decision 'Aircraft Cybersecurity'	EASA decision adding cybersecurity requirements to all Certification Specification which includes need for

² As current in e-CFR as of May 7, 2020 equivalent to Amendment 21-100

³ Ibid.

⁴ Ibid.

⁵ AMC20-152A has been issued but the equivalent AC20-152A has not been issued yet but release is imminent in 2020. See

https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/planned/

		applicants to provide evidence of security measures and verification in products
AMC 20-42	EASA - General Acceptable Means of Compliance for Airworthiness of Products, Parts, and Appliances	Provides European Union Aviation Safety Agency (EASA) Guidance for Airworthiness Information Security Risk Assessments
EASA Certification Specification CS-25, Subpart F – Equipment (CS 25.1319)	EASA “Easy access Rules for Large Aeroplane” (CS-25), CS 25-1319 - Equipment, systems and network protection	Requires aeroplane equipment, systems and networks be protected from intentional unauthorized electronic interactions that may result in adverse effects to the safety of the aeroplane.
FAA Order 1600.75 [Note: Restricted Controlled Document]	Protecting Sensitive Unclassified Information (SUI)	Provides FAA guidance and requirements for protecting Sensitive Unclassified Information (SUI)

Table 2 Standards supporting airplane testing requirements

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
EUROCAE ED-12C (equivalent to RTCA DO-178C)	Software Considerations in Airborne Systems and Equipment Certification	Provides guidance and compliance objects for developing airborne software
EUROCAE ED-80 (equivalent to DO-254)	Design Assurance Guidance for Airborne Electronic Hardware	Provides guidance and compliance objectives for developing airborne hardware
EUROCAE ED-202A (equivalent to RTCA DO-326A)	Airworthiness Security Process Specification	Provides guidance on secure development of aircraft and aircraft systems
EUROCAE ED-203A (equivalent to RTCA DO-356A)	Airworthiness Security Methods and Considerations	Provides methods and compliance objectives to securely develop aircraft and aircraft systems
RTCA DO-178C (equivalent to EUROCAE ED-12C)	Software Considerations in Airborne Systems and Equipment Certification	Provides guidance and compliance objects for developing airborne software
RTCA DO-254 (equivalent to EUROCAE ED-80)	Design Assurance Guidance For Airborne Electronic Hardware	Provides guidance and compliance objectives for developing airborne hardware
RTCA DO-326A (equivalent to EUROCAE ED-202A)	Airworthiness Security Process Specification	Provides guidance on secure development of aircraft and aircraft systems
RTCA DO-355A (equivalent to EUROCAE ED-204)	Information Security Guidance for Continued Airworthiness	Provides methods and compliance objectives for information security relating aircraft and ground systems

RTCA DO-356A (<i>equivalent to EUROCAE ED-203A</i>)	Airworthiness Security Methods and Considerations	Provides methods and compliance objectives to securely develop aircraft and aircraft systems
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.

8 Abbreviations

AC	Advisory Circular
AIA	Aerospace Industries Association
A-ISAC	Aviation Information Sharing and Analysis Center
AMC	Acceptable Means of Compliance
ARP	Aerospace Recommended Practice
AS	Aerospace Standard
ASD	AeroSpace and Defence Industries Association of Europe
CFR	Code of Federal Regulation
COTS	Commercial-Off-The-Shelf
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
DAL	Design/Development Assurance Level
DOC	Document
EASA	European Aviation Safety Agency
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
GAO	General Accounting Office (US)
GDPR	General Data Privacy Regulation (EU)
HW	Hardware
IAQG	International Aerospace Quality Group
ICAO	International Civil Aviation Organisation
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
ISO	International Organization for Standardization
LRU	Line Replaceable Unit
MRO	Maintenance, Repair or Overhaul
OEM	Original Equipment Manufacturer
OpSpec	Operational Specification
RMT	Rulemaking Task
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automobile Engineers
SAL	Security Assurance Level
STD	Standard
SW	Software

9 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 Title 14 of the Code of Federal Regulations (14 CFR): Regulations (14 CFR) parts 121, 121/135, 125
14 CFR Part 121	Operating requirements: domestic, flag, and supplemental operations
14 CFR Part 125	Certification and operations: airplanes having a seating capacity of 20 or more passengers or a maximum payload capacity of 6,000 pounds or more; and rules governing persons on board such aircraft
14 CFR Part 129	Operations: foreign air carriers and foreign operators of U.S.-registered aircraft engaged in common carriage
14 CFR Part 135	Operating requirements: commuter and on demand operations and rules governing persons on board such aircraft
49 CFR Part 15	Protection of Sensitive Security Information
49 CFR Part 1520	Protection of Sensitive Security Information
AC 20-152A / AMC 20-152A	Development Assurance for Airborne Electronic Hardware
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
ANSOG	Airplane Network Security Operator Guidance (ANSOG) for 737, 747, 767, 777, 787 (All Models)
Commission Regulation (EU) No 748/2012 (<i>EASA Part 21</i>)	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) No 679/2016 (<i>GDPR</i>)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
CVSSv3.1	Common Vulnerability Scoring System version 3.1 Specification Document
EASA NPA 2019-07	Management of Information Security Risks
ED Decision 2020/006/R	Executive Director Decision 'Aircraft Cybersecurity'
EUROCAE ED-12B (<i>equivalent to RTCA DO-178B</i>)	Software Considerations in Airborne Systems and Equipment Certification
EUROCAE ED-12C (<i>equivalent to RTCA DO-178C</i>)	Software Considerations in Airborne Systems and Equipment Certification

EUROCAE ED-202A (<i>equivalent to RTCA DO-326A</i>)	Airworthiness Security Process Specification
EUROCAE ED-203A (<i>equivalent to RTCA DO-356A</i>)	Airworthiness Security Methods and Considerations
EUROCAE ED-204A (<i>equivalent to RTCA DO-355A</i>)	Information Security Guidance for Continuing Airworthiness
EUROCAE ED-79A (<i>equivalent to SAE ARP 4754A</i>)	Guidelines for Development of Civil Aircraft and Systems
EUROCAE ED-80 (<i>equivalent to DO-254</i>)	Design Assurance Guidance for Airborne Electronic Hardware
EUROCAE ED-ISEM (<i>equivalent to RTCA DO-ISEM, reference number not yet issued</i>)	Information Security Event Management
FAA OpSpec D301	FAA OpSpec D301, Aircraft Network Security Program (ANSP) dated 31 May 2012
FAA Order 1600.75	Protecting Sensitive Unclassified Information (SUI)
FAA Order 8110.105A	Simple and Complex Electronic Hardware Approval Guidance
FAA Order 8110.49 Chg 1	Software Approval Guidelines
GAO Report GAO-21-86	Aviation Cybersecurity FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks
ISO 9001:2015	Quality management systems - Requirements
RTCA DO-178B (<i>equivalent to EUROCAE ED-12B</i>)	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-178C (<i>equivalent to EUROCAE ED-12C</i>)	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-254 (<i>equivalent to EUROCAE ED-80</i>)	Design Assurance Guidance For Airborne Electronic Hardware
RTCA DO-326A (<i>equivalent to EUROCAE ED-202A</i>)	Airworthiness Security Process Specification
RTCA DO-355A (<i>equivalent to EUROCAE ED-204A</i>)	Information Security Guidance for Continuing Airworthiness
RTCA DO-356A (<i>equivalent to EUROCAE ED-203A</i>)	Airworthiness Security Methods and Considerations
RTCA DO-ISEM (<i>equivalent to EUROCAE ED-ISEM, reference number not yet issued</i>)	Information Security Event Management
SAE ARP 4754A (<i>equivalent to EUROCAE ED-79A</i>)	Guidelines for Development of Civil Aircraft and Systems
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

