U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: Aircraft Systems Information Security Protection (ASISP)

Date: D R A F T **AC No:** 20-XXX
Initiated By: AIR-600

1 **PURPOSE.**

This advisory circular (AC) provides guidance to address aircraft systems information security/protection (ASISP) for compliance under title 14, Code of Federal Regulations (14 CFR) 25.1319, 33.28, and 35.23 and their associated appendices. These requirements provide a regulatory basis for protection from intentional attacks on transport category airplanes, engines, and propellers.

2 **APPLICABILITY.**

2.1 The guidance in this AC is for airplane, engine and propeller manufacturers; modifiers, foreign regulatory authorities, Federal Aviation Administration (FAA) type certification engineers, FAA Flight Standards personnel, and the Administrator's designees.

2.2 The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This AC is intended only to provide information to the public regarding existing requirements under the law or agency policies. Conformity with the guidance is voluntary only and nonconformity will not affect rights and obligations under existing statutes and regulations. This AC describes an acceptable means, but not the only means, for showing compliance with §§ 25.1319, 33.28, and 35.23. Terms such as "should," "shall," "may," and "must" are used only in the sense of ensuring applicability of this particular method of compliance when the acceptable method of compliance in this document is used. The FAA will consider other methods of demonstrating compliance that an applicant may elect to present. If the FAA becomes aware of circumstances in which following this AC would not result in compliance with the applicable regulations, the agency may require additional substantiation as the basis for finding compliance.

2.3 The material in this AC does not change, create any additional, authorize changes in, or permit deviations from existing regulatory requirements.

3 RELATED DOCUMENTS.

3.1 Regulations.

The following regulations are related to this AC. The full text of these regulations can be downloaded from the U.S. Government Publishing Office e-CFR. A paper copy can be ordered from the Government Publishing Office, Superintendent of Documents, Attn: New Orders, PO Box 371954, Pittsburgh, PA, 15250-7954A.

- Section 25.1301, *Function and installation*.
- Section 25.1309, *Equipment, systems, and installations.*
- Section 25.1319*, Equipment, systems, and network information security protection.*
- Section 25.1529, *Instructions for Continued Airworthiness*.
- Appendix H to Part 25, *Instructions for Continued Airworthiness.*
- Section 33.28, *Engine control systems*.
- Section 33.4, *Instructions for Continued Airworthiness*.
- Appendix A to Part 33, *Instructions for Continued Airworthiness.*
- Section 35.23, *Propeller control system*.
- Section 35.4, *Instructions for Continued Airworthiness*.
- Appendix A to Part 35, *Instructions for Continued Airworthiness.*

3.2 Advisory Circulars.

The following ACs are related to the guidance in this AC. If any AC is revised after publication of this AC, you should refer to the latest version on the FAA website at www.faa.gov/regulations_policies/advisory_circulars/.

- AC 20-115D, *Airborne Software Assurance*, dated July 21, 2017.
- AC 119-1A, *Operational Authorization of Aircraft Network Security Program (ANSP)*, dated September 28, 2023.
- AC 20-152A, *Development Assurance for Airborne Electronic Hardware*, dated October, 7, 2022.
- AC 20-153B, *Acceptance of Aeronautical Data Processes and Associated Databases*, dated April 19, 2016.

3.3 Industry Standards.

- *A Report from the Aviation Rulemaking Advisory Committee (ARAC) Aircraft System Information Security / Protection (ASISP) working group to the Federal Aviation Administration*, dated August 22, 2016, www.faa.gov/regulations_policies/rulemaking/committees/documents/media/ARACasisp-T1-20150203R.pdf..

- National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, dated February 12, 2014.
- RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 13, 2011.
- EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 2012.
- RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, dated April 19, 2000.
- EUROCAE ED-80, *Design Assurance Guidance for Airborne Electronic Hardware*, dated April 2000.
- RTCA DO 326A, *Airworthiness Security Process Specification,* dated August 6, 2014.
- EUROCAE ED-202A, *Airworthiness Security Process Specification,* dated June 2014.
- RTCA DO-355A, *Information Security Guidance for Continuing Airworthiness*, dated September 10, 2020.
- EUROCAE ED-204A, *Information Security Guidance for Continuing Airworthiness*, dated September 14, 2020.
- RTCA DO-356A, *Airworthiness Security Methods and Considerations*, dated June 21, 2018.
- EUROCAE ED-203A, *Airworthiness Security Methods and Considerations*, dated June 8, 2018.
- RTCA DO-391, *Aeronautical Information Systems Security Framework Guidance,* dated December 16, 2021.
- EUROCAE ED-201A, *Aeronautical Information Systems Security Framework Guidance,* dated December 17, 2021.
- RTCA DO-392, *Guidance on Security Event Management*, dated June 23, 2023.
- EUROCAE ED-206, *Guidance on Security Event Management*, dated June 28, 2023.
- SAE, Aerospace Recommended Practice ARP 4754a, *Guidelines for Development of Civil Aircraft and Systems*, dated December 21, 2010.
- SAE, Aerospace Recommended Practice ARP 4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, dated December 1, 1996.
- SAE AIR7368 – *Cybersecurity for Propulsion Systems*, dated September 5, 2023.

Note: EUROCAE ED is hereafter referred to as ED; RTCA DO is hereafter referred to as DO. Where the notation ED-XXX/DO-XXX appears in this document, the referenced documents are recognized as being equivalent.

4 BACKGROUND.

The current trend in system design is an increasing level of integration between airplane, engine, and propeller systems with increased connectivity to internal and external data networks. The cybersecurity threat environment is one that rapidly changes and requires constant monitoring to identify and mitigate new threat sources. These designs can introduce ASISP vulnerabilities.

Note: "ASISP" and "Information Security" are terms that are used interchangeably in this AC and related industry standards.

5 GUIDANCE FOR THE USE OF THIS AC.

5.1 What this AC Applies to.

This AC applies to initial type certificate (TC), supplemental type certificate (STC), amended TC, or amended STC applications for aircraft, aircraft systems, and aircraft engine and propeller systems connecting to any internal or external data networks and services. The following are examples of networks and services:

- Field loading of software;
- Maintenance laptops;
- Airport/airline Gatelinks;
- Public networks, e.g., Internet;
- Wireless aircraft sensors and sensor networks;
- Cellular networks;
- Universal serial bus (USB) devices;
- Satellite communications;
- Portable electronic devices and portable electronic flight bags (EFBs);and
- GPS and satellite-based augmentation system (SBAS) digital data.

5.2 What is Outside the Scope of this AC.

This AC does not apply to aeronautical databases or the Aircraft Communications Addressing and Reporting System (ACARS)provided data security and integrity checks are in place. If those checks are not in place, the security risk assessment and mitigations of §§ 25.1319(a), 33.28(n), and 35.23(f) should account for the links to aeronautical databases and ACARS as applicable; and the information security guidance in this AC applies.

Overall guidance for aeronautical databases and ACARS is provided in:

- FAA AC 20-153B, *Acceptance of Aeronautical Data Processes and Associated Databases*, dated April 19, 2016
- RTCA DO-200C *Standards for Processing Aeronautical Data,* dated *June 27, 2024* .
- FAA AC 90-117 *Data Link Communications*, dated October 3, 2017
- ARINC 633-5 *AOC Air-Ground Data and Message Exchange Format*, dated January 9, 2024
- ARINC 618-9 *Air/Ground Character-Oriented Protocol Specification,* dated *July 17, 2023*
- ARINC 723P1- *Datalink Security – ACARS Message Security*, dated December 10, 2007
- ARINC 723P2 – *Datalink Security – Key Management*, dated March 10, 2008

6 FIELD LOADABLE SOFTWARE (FLS).

The software loading function, including support systems and procedures, should include a means to detect any anomaly in the loading process. As part of compliance with the requirements in §§ 25.1319(a), 33.28(n), and 35.23(f) to identify and assess certain security risks, and the ICA provisions of §§ H25.1, H25.3, A33.3(a)(10), and A35.3(a)(10), a security risk analysis is necessary for new data loading systems and major modifications to existing systems. Additional policy and guidance for security considerations of EFB systems are described in the following ACs: AC 20-173A, *Installation of Electronic Flight Bag Components*, and AC 120-76D, *Authorization for Use of Electronic Flight Bags*. Applicants should ensure they are meeting requirements of §§ 25.1309, 33.28, 35.23 for field-loadable software (Reference AC 20-115D, *Airborne Software Development Assurance Using ED-12() and DO-178().*

7 MEANS OF COMPLIANCE FOR ASISP.

Applicants are encouraged to use RTCA information security documents to show compliance with §§ 25.1319, 33.28(n), 35.23(f) for ASISP. These documents address failure modes associated with electronic access points, where the security of the system interfaces, or information crossing these interfaces, may cause or contribute to failures that may impact aircraft safety. This AC recognizes the current version of the following RTCA documents as an acceptable method of compliance for the ASISP aspects of § 25.1319, and for the §§ 33.28(n) and 35.23(f) requirements for engines and propellers. intended for part 25 airplane installation. For engines and propellers on other installations, other industry guidance (such as ASTM F3532-22, *Protection of Aircraft Systems from Intentional Unauthorized Electronic Interactions)* may be used as a method of compliance for §§ 33.28(n) and 35.23(f), in accordance with applicable FAA guidance.

In addition, for engines and propellers for all aircraft installations, SAE AIR7368 is recognized as supplementary guidance on application of the RTCA and other industry documents to cybersecurity for engine and propeller control and monitoring systems.

7.1 **DO-326A/ED-202A, Airworthiness Security Process Specification.**

This document provides process assurance guidance and requirements for the aircraft design regarding systems information security.

7.2 **DO-355A/ED-204A, Information Security Guidance for Continuing Airworthiness.**

This document provides guidance for assuring continued safety of aircraft in service regarding systems information security.

7.3 **DO-356A/ED-203A, Airworthiness Security Methods and Considerations.**

This document provides analysis and assessment methods for executing the process assurance specified in DO-326A/ED-202A.

Note: The definitions for development assurance level and security assurance level are defined in the above RTCA documents.

7.4 **DO-391/ED-201A, Aeronautical Information System Security Framework Guidance.**

This document provides context of the shared responsibility for aeronautical information system security (AISS) through the identification and description of topics to be addressed.

7.5 **DO-392/ED-206, Guidance on Security Event Management.**

This document provides guidance on security event management for various stakeholders in the aviation environment such as manufacturers, operators, maintainers, product suppliers, service providers, etc., to develop processes and procedures for identifying, responding to, and reporting information security events impacting aviation safety.

8 GUIDANCE FOR THE USE OF THE RTCA INFORMATION SECURITY DOCUMENTS.

8.1 Where the applicant intends to use the RTCA information security documents listed in paragraphs 7.1 through 7.5 of this AC as a means of compliance, the FAA encourages the applicant to coordinate with the FAA early in the project development process.

8.2 Where the applicant intends to propose the use of methods of compliance other than the RTCA information security documents (see paragraphs 7.1 through 7.5 of this AC), the applicant should discuss that intention with the FAA early in the project development process.

8.3 The SAE AIR 7368 report, *Cybersecurity for Propulsion Systems*, may be used as supplementary guidance on application of the RTCA and other industry documents to cybersecurity for engine and propeller control and monitoring systems.

9 SUGGESTIONS FOR IMPROVING THIS AC.

If you have suggestions for improving this AC, you may use the Advisory Circular Feedback Form at the end of this AC.

OMB Control Number: 2120-0746
Expiration Date: 11/30/2024

Advisory Circular Feedback

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) emailing this form to (9-AWA-AVS-AIR-DMO@faa.gov) or (2) faxing it to the attention of the LOB/SO _____N/A_____.

Subject:_____ Date: _____

Please mark all appropriate line items:

☐ An error (procedural or typographical) has been noted in paragraph_____on page_____.

☐ Recommend paragraph_____on page_____be changed as follows:

☐ In a future change to this AC, please cover the following subject: *(Briefly describe what you want added.)*

☐ Other comments:

☐ I would like to discuss the above. Please contact me.

Submitted by:_____Date: _____