RTCA, Inc.
1150 18th Street, NW, Suite 910
Washington, DC 20036, USA

Report on Aviation Data Security

RR-005
June 26, 2025

Prepared by: SC-216
©2025 RTCA, Inc.

Copies of this document may be obtained from:

RTCA, Inc.
1150 18th St. NW, Suite 910
Washington, D.C. 20036, USA

Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org

Please call RTCA for price and ordering information.

FOREWORD

This document was prepared by Special Committee 216 (SC-216) with EUROCAE Working Group 72 (WG-72) and approved by the RTCA Program Management Committee (PMC) on June 26, 2025 and the EUROCAE Secretariat on July 2, 2025.

RTCA, Incorporated is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization develops consensus-based recommendations on contemporary aviation issues. RTCA's objectives include but are not limited to:

- coalescing aviation system user and provider technical requirements in a manner that helps government and industry meet their mutual objectives and responsibilities;

- analyzing and recommending solutions to the system technical issues that aviation faces as it continues to pursue increased safety, system capacity and efficiency;

- developing consensus on the application of pertinent technology to fulfill user and provider requirements, including development of minimum operational performance standards for electronic systems and equipment that support aviation; and

- assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunication Union and other appropriate international organizations can be based.

The organization's recommendations are often used as the basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration Technical Standard Orders and several advisory circulars.

Since RTCA is not an official agency of the United States Government, its recommendations may not be regarded as statements of official government policy unless so enunciated by the U.S. government organization or agency having statutory jurisdiction over any matters to which the recommendations relate.

DISCLAIMER

This publication is based on material submitted by various participants during the SC approval process. Neither the SC nor RTCA has made any determination whether these materials could be subject to valid claims of patent, copyright or other proprietary rights by third parties, and no representation or warranty, expressed or implied is made in this regard. Any use of or reliance on this document shall constitute an acceptance thereof "as is" and be subject to this disclaimer.

This Page Intentionally Left Blank

TABLE OF CONTENTS

1 SCOPE 1

1.1 Introduction 1
1.2 Scope & Approach 1
1.3 How To Use This Report 2
1.4 Assumptions 2
1.5 Future Scope 2

2 AVIATION DATA LIFE CYCLE 3

2.1 Aviation Ecosystem Data 3
2.2 Data Security Life Cycle 4
2.2.1 Defining Aviation Data Security 4
2.2.2 Data Security Life Cycle Phases 5
2.2.3 Product Security Life Cycle Stages 6

3 AVIATION DATA SECURITY FRAMEWORK 9

3.1 Framework Introduction 9
3.2 Data and Stakeholder identification 9
3.2.1 Data Identification 10
3.2.2 Stakeholder Identification 11
3.3 Data flow & interfaces determination 13
3.4 Data Protection 14
3.4.1 Safety Effect and Information Security Attributes 14
3.4.2 Information Security Requirements 14
3.4.3 Develop and Implement Information Security Methods and Control 15
3.4.4 Information Security Methods, Compliance Assessment and Remediation 15

4 AIRBORNE SOFTWARE SECURITY MEASURES 17

4.1 Overview 17
4.2 Scope 17
4.3 Out of Scope 17
4.4 Secure Loading and Secure Distribution 18
4.5 Security Recommendations 18

5 MEMBERSHIP 21

APPENDIX A ACRONYMS & REFERENCES A-1

A.1 Definitions A-1
A.2 Reference Documents A-1

APPENDIX B AIRBORNE SOFTWARE LOADING FIGURES B-1

B.1 Overview B-1

TABLE OF TABLES

Table 3-1: A Sample Table of Data Assets 10
Table 3-2: A Sample Requirements Traceability MatRIX 10
Table 3-3: A Sample Table of Data Assets With Stakeholders 12

TABLE OF FIGURES

Figure 1-1: NIST CSF 2.0 Functions 1
Figure 2-1: Aviation Data security life cycle 4
Figure 2-2: CIA Triad 5
Figure 2-3: An Example of an Aviation Product Security Life Cycle 7
Figure 3-1: Aviation Data Security Framework 9
Figure 3-2: An Example Data Life cycle Diagram with Stakeholders 13

1 SCOPE

1.1 Introduction

This report is the joint product of two industry committees: the EUROCAE Working Group WG-72, "Aeronautical Systems Security," and the RTCA Special Committee SC-216, "Aeronautical Systems Security." Both committees agreed that the information provided by this report address the increasing potential for Intentional Unauthorized Electronic Interaction (IUEI) with aircraft information systems.

1.2 Scope & Approach

The aviation ecosystem consists of many complex systems that span information technology (IT) and operational technology (OT). A blended approach of IT and OT security methods are required to adequately meet the rapidly changing threat landscape. The attributes of confidentiality, integrity, and availability in addition to system specific information security methods can be considered to provide robustness.

The scope of this informative report consists of three main sections. First is to define an aviation focused data security life cycle. Second is to develop an aviation data security framework for regulatory and standards groups to utilize to create aviation security objectives. Third is to provide recommendations on sufficient security measures for airborne software.

The proposed data life cycle focuses on how data transverses in the aviation ecosystem. Associated examples identify how data is generated, transported, stored, used, and decommissioned between multiple stakeholders of the aviation ecosystem. Data categorization provides a baseline of how data is secured based on overall system risk and data characterization. Since multiple stakeholders touch aviation data throughout its life cycle, objectives identify which stakeholders are responsible for data security during specific life cycle phases. Chapter 3 of this report contains guidance on how to develop those objectives.

Like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), as displayed in Figure 1.1, [Reference A.2.1], the aviation data security framework leverages similar functions. The focus of the aviation data security framework is primarily on the Identify and Protect functions. For more information regarding the govern function, refer to ED-201A/DO-391 [Reference A.2.15]. For the Detect/Respond/Recover functions, refer to ED-206/DO-392 [Reference A.2.18].

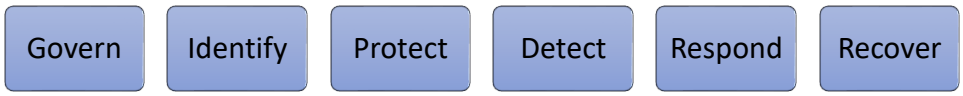


Figure 1-1: NIST CSF 2.0 Functions

For specific implementations of protecting data on the aircraft, please refer to ED-202B/DO-326B [Reference A.2.12] and ED-203A/DO-356A [Reference A.2.14]. For protecting data within air traffic management systems, please refer to ED-205A/DO-393 [Reference A.2.17]. For specific implementation of protecting data for continuing airworthiness, please refer to ED-204A/DO-355A [Reference A.2.13].

 ©RTCA, Inc 2025

The intent is to utilize the framework defined in this report to adequately secure airborne software.

1.3 How To Use This Report

For individuals who participate in regulatory and standards organizations, the intent of the framework defined in Section 3 is to allow users to capture minimum and consistent security objectives for data protection within the aviation ecosystem. Misuse of aviation data might lead to information security threats including impacts to human and equipment safety. The framework is meant to be utilized for new and existing data types or constructs to provide effective security and assurance for the data.

For individuals who need to secure airborne software, a list of recommendations is provided for the scope defined in Section 4.2. The recommendations are not a formal means of compliance (MOC).

1.4 Assumptions

Readers of this report need to have foundational knowledge of information security and an architectural understand of the aviation ecosystem and its stakeholders. Advanced knowledge of product security notions, IT versus OT concepts and aviation stakeholder roles will aid in better understanding the use cases provided in the appendices. Knowledge of aviation regulation aids in the understanding of implementation timelines of the guidance provided in this report.

1.5 Future Scope

Standards will be needed to define the information security objectives and requirements for aviation data. It is recommended to utilize the information in this report and gather feedback from the aviation community to develop standards as necessary.

Topics deemed as important for future discussions include but are not limited to:

- Minimum security recommendations for database production systems
- Minimum security recommendations for Raw Data Suppliers of database systems
- Minimum security recommendations for cryptography for aviation systems

2 AVIATION DATA LIFE CYCLE

2.1 Aviation Ecosystem Data

The aviation data ecosystem is comprised of multiple data types. The focus of this report is data in the ecosystem that could have an impact on safety of flight.

The existing aviation safety standards and regulatory requirements contain guidance aimed at reducing the likelihood of an aviation accident. With it, an accident or serious incident would only happen in the event of several deficiencies happening simultaneously and, by chance, aligning themselves. Authorities have raised concern that the possibility of vulnerabilities in different organizations which can be aligned and exploited by individuals with a malicious intent. The risk is constantly increasing in the civil aviation ecosystem as aeronautical information systems become more and more connected. Several major components interacting with the aircraft, as well as with each other, require functional data exchanges that need to be protected since they have consequences on the safety of flight.

The identification of these risks must consider that there are threat actors with intent and desire to damage aviation systems, disrupt operations, or threaten human lives. In other words, they are looking for vulnerabilities in the ecosystem to exploit to create harm. The manipulation of data through IUEI with aircraft systems is one means to achieve this goal.

IUEI is defined as "a circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces .” [Reference A.2.12] The goal is to ensure that the airworthiness of an aircraft is not compromised from IUEI.

The scope of data security within the aviation ecosystem includes all electronic data that is subject to IUEI in including known and future data types that impact aviation safety.

1. Paper and analog data is out of scope.
2. Paper and analog data may be converted to digital and then would fall within scope.

To better define data, the following definitions include but are not limited to:

- DO-200C/ED-76B: "Data used for aeronautical applications such as navigation, flight planning, flight simulators, terrain awareness, and other purposes (e.g., navigation data, terrain and obstacle data, and aerodrome mapping data). "
- NISTIR 4734: "A representation of information as stored or transmitted."
- NIST Privacy Framework V1.0: " A representation of information, including digital and non-digital formats".

Data is any information that impacts aircraft functionality via IUEI. Examples of data that may affect the aircraft functionality, and maintainability in relation to safety that are also subject to IUEI include but are not limited to:

- Airborne Software
- Aircraft Logs
- Airborne Databases
- Maintenance Data

 ©RTCA, Inc 2025

- Production Data
- Airborne System Compliance Data
  - i.e. test and production data, design data
- Private keys used for integrity / authenticity checks

2.2 Data Security Life Cycle

Aviation ecosystem data moves through multiple phases during its life cycle. Each phase has security aspects that can apply. This report uses the following four phases as referenced by NIST and displayed in Figure 2.1:

- Identify: organization identifies and categorizes the data (Creation)
- Use: organization accesses, views, shares, or modifies data by aggregating (merging data) or disaggregating (breaking data) or repurposing via additional usage and sharing
- Maintain: organization preserves the data during its life span including the storage and archiving of any data
- Dispose: organization disposes or destroys the data at the end of its life span

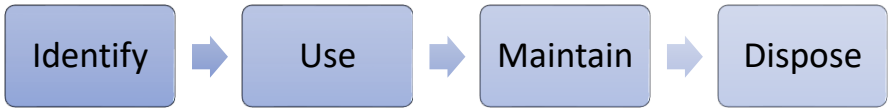


Figure 2-1: Aviation Data security life cycle

Note: Airborne data interactions in aviation certified systems may have system security design requirements covered by appropriate standards.

2.2.1 Defining Aviation Data Security

The following sections cover the life cycle of data as it could transition through an aviation-related system. The Confidentiality, Integrity and Availability security (CIA) triad model, as displayed in Figure 2.2 [Reference A.2.2], is used to highlight the fundamental security attributes of concern. The CIA model refers to:

- Confidentiality – the attribute on the effect of losing "restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."
- Integrity — the attribute on the effect of losing "improper information modification or destruction and ensuring information non-repudiation and authenticity."
- Availability – the attribute on the effect of losing "timely and reliable access to and use of information."