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

Aeronautical Information System Security Framework Guidance

RTCA DO-391
December 16, 2021

Prepared by: SC-216
© 2021 RTCA, Inc.

Copies of this document may be obtained from
RTCA, Inc.
Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org
Please visit the RTCA Online Store for document pricing and ordering information.

FOREWORD

This document was prepared by Special Committee 216 (SC-216) Aeronautical Information Systems Security jointly with EUROCAE Working Group 72 (WG-72) and approved by the RTCA Program Management Committee (PMC) and the EUROCAE Council on December 16, 2021.

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 functions as a Standards Development Organization and 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 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 INTRODUCTION 1

1.1 Purpose 1
1.2 Scope 1
1.3 Document Structure 3
1.4 Conventions of this Document 3
1.5 Relationship to Other Documents 4

2 CONCEPTS AND FRAMEWORK 5

2.1 Aviation Security Environment and Evolution 5
2.1.1 Aviation Stakeholder Framework 5
2.1.2 Product Life-Cycle 7
2.1.3 Transition Between Life-Cycle Phases 10
2.1.4 Evolution of Technology and Attacks 12
2.1.5 Security Environment 15
2.2 Risk Management and Assurance 15
2.2.1 Risk Management 15
2.2.2 Assurance 32
2.3 Supply Chain 36

3 GUIDANCE MATERIAL ON AVIATION INFORMATION SECURITY MANAGEMENT SYSTEMS 39

3.1 Overview and Objectives 39
3.2 Information Security Management System (ISMS) 39
3.2.1 Overview 39
3.2.2 Scope 40
3.2.3 Overview and Structure of This Guidance 40
3.3 Aviation Organization ISMS Objectives 41
3.3.1 Security Policies, Processes 41
3.3.2 Framework for Risk Management 41
3.3.3 Information Security Monitoring and Reporting Framework 42
3.3.4 Personnel Training and Skills 42

3.3.5 Information Security Management Manual 42
3.3.6 Record Keeping 42
3.3.7 Continuous Monitoring and Improvement of ISMS Framework 43
3.4 Assurance 43
3.4.1 Assurance in the Aircraft Ecosystem Case 43
3.4.2 Assurance in the ANSP Ecosystem Case 44

4 RISK ASSESSMENT AND INFORMATION SHARING 49

4.1 Security Risk Assessment Criteria and Output Comparability 49
4.1.1 Introduction 49
4.1.2 Risk Assessment and Sharing Criteria 49
4.1.3 Security Risk Assessment Comparability Principles 57
4.2 Information Sharing 58
4.3 Assurance Mapping 58
4.4 External Agreements 58
4.4.1 Statements for Agreements 59
4.4.2 External Agreement for Information Security 60

5 INDUSTRY BEST PRACTICES 61

5.1 Threat Intelligence 61
5.2 Disposal of Assets 62
APPENDIX A : COMPARING THE ISO 27005 FRAMEWORK, ICAO Global Risk Context Statement AND NIST SP 800-30 PROCESS A-1
APPENDIX B : TEMPLATES AND CLASSIFICATIONS B-1
B.1 External Agreement for Security Clauses B-1
B.1.1 Full Template B-1
B.2 Security Risk Assessment Sharing Template B-4
B.3 Risk Assessment Classifications B-7
B.3.1 Risk Acceptance Comparison Matrix B-7
B.3.2 Severity of the Threat Condition Classification – Safety B-8
B.3.3 Level of Threat Classification B-11
B.3.4 Security Risk Assessment – Capacity B-12
B.3.5 Risk Assessment Assurance Objectivities B-12
B.4 Aviation Organization ISMS Objectives B-13
B.5 Security Assurance Mapping – Examples Of Ecosystem Data Exchanges B-14
APPENDIX C : CASE STUDIES C-1
C.1 Example for Case Study C-1

C.1.1 Connected Interfaces C-1
C.1.2 Organization Individual SRA C-1
C.1.3 Organization C Assess the Outputs of the SRA's C-10
C.2 RASCI Example C-13
APPENDIX D : GLOSSARY D-1
APPENDIX E : ACRONYMS AND ABBREVIATIONS E-1
APPENDIX F : REFERENCES F-1
APPENDIX G : USAGE OF AND RELATION WITH OTHER EUROCAE AND RTCA DOCUMENTS G-1
APPENDIX H : REVISION GUIDE H-1
APPENDIX I : MEMBERSHIP I-1

LIST OF FIGURES

Figure 2-1: Relationships Between Stakeholders 7
Figure 2-2: Relationship of Life-Cycle Phases of Separate Products 11
Figure 2-3: Impact and Required Attack Capability Over Time 14
Figure 2-4: ED-76A/ DO-200B – Aeronautical Data Chain Participants and Flow of Aeronautical Data. 21
Figure 2-5: Aeronautical Organisations and Flow of Aeronautical Information System Security 22
Figure 2-6: Oversight Process Cycle for Shared Risks 23
Figure 2-7: Threat Information Categories 25
Figure 2-8: High Level View of Connected Ecosystems 26
Figure 2-9: Scope of Assurance Between Stakeholders 35
Figure 3-1: Example of Ecosystem 47
Figure 4-1: Risk Assessment and Sharing Stages 50

Figure C- 1: Case Study Example Connected Organizations C-1
Figure C- 2: Organization A Threat Scenarios C-2
Figure C- 3: Organization B Threat Scenarios C-4
Figure C- 4: Organization C Threat Scenarios C-7

LIST OF TABLES

Table 2-1: Examples for Assurance Methods (From ISO/IEC Tr 15443- 1:2012) 33
Table 2-2: Overview of The Associated Implementing Rules and Their Means of Compliance/ Assurance 36

Table 3-1: Examples of Assurance Objectives on Data Exchanged in the Aircraft Ecosystem 44
Table 3-2: Examples of Assurance Objectives on Data Exchanged in the ANSP (Air Navigation Service Provider) Ecosystem 45

Table B-1: External Agreement Template B-1
Table B-2: External Agreement Template - Contractual B-3
Table B-3: SRA Sharing Template B-4
Table B-4: Comparison Risk Acceptance Matrix B-8
Table B-5: Severity of Threat Condition Classification-Aircraft B-8
Table B-6: Severity of Threat Condition Classification-ATM/ANS B-9
Table B-7: Severity of Threat Condition Classification-Airspace/CNS B-9
Table B-8: Severity of Threat Condition Mapping Example B-10
Table B-9: Level of Threat Classification- Safety B-11
Table B-10: Level of Threat Mapping Example B-12
Table B-11: ED-205A/DO-393 Mapping B-12
Table B-12: Risk Assessment Assurance Objectives B-12
Table B-13: Aviation Organization ISMS Objectives B-13
Table B-14: Examples of Data Exchanged Between Ecosystems B-15

Table C-1: Organization A Risk Assessment C-2
Table C-2: Organization A Mapping To ED-201A/DO-391 ..... C-2
Table C-3: Organziation A SRA Template C-3
Table C-4: Organization B Risk Assessment C-5
Table C-5: Organization B Mapping To ED-201A/DO-391 ..... C-5
Table C-6: Organization B SRA Template C-5
Table C-7: Organization C Risk Assessment C-7
Table C-8: Organization C Mapping To ED-201A/DO-391 ..... C-8
Table C-9: Organization C SRA Template C-8
Table C-10: Assessment of the Outputs of the SRA's C-10
Table C-11: RASCI Example Incident Handling C-13

This Page Intentionally Left Blank

1 INTRODUCTION

This document is the joint product of two industry committees: the EUROCAE Working Group WG-72, titled "Aeronautical Information Systems Security" and the RTCA Special Committee SC-216, also titled "Aeronautical Information Systems Security". WG-72 was formed to address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment, while SC-216 was formed more specifically to address information security for certification of aircraft and its systems. Both committees agreed that the guidance provided by this document and its companion documents constitute aviation best practices to address the increasing potential for Intentional Unauthorized Electronic Interaction (IUEI) with aeronautical information systems. Both committees agree that the guidance is suitable for use as acceptable means of compliance in relevant jurisdictions. For a discussion of the usage of ED-201A/DO-391 and its relation with other EUROCAE/RTCA documents please see Appendix G. Appendix H provides a revision guide of the major changes to the ED-201 document, which was a sole publication of EUROCAE.

1.1 Purpose

This document is concerned with the overarching context of the shared responsibility for AISS through the identification and description of topics which have to be addressed. It deals with shared responsibility of all relevant stakeholders who are part of civil aviation. The purpose of security in this context should be understood as ensuring safety of flight and maintaining the operation of the civil aviation infrastructure without significant disruption.

1.2 Scope

The AISS guidance in this document may be used to address relevant aviation areas including:

- Aircraft design and production and aircraft components,
- Aircraft operations, maintenance repair and overhaul operations (MRO) and airports,
- Air Traffic Management (ATM) which includes but is not limited to the assets, resources that are used in the operations and delivery of Performance Based Navigation (PBN) and Performance Based Communication and Surveillance (PBCS) and Aviation Service Providers (ASP),
- Unmanned Aerial Systems (UAS) and Unmanned Aircraft System Traffic Management (UTM) operations and organizations that provide or exchange information that have an impact to ATM (Air Traffic Management) automation systems or human resources and the decision making processes for ATM or aircraft operations (such as NOTAMS (Notices to Airmen), weather, obstacles, routes & restrictions, manuals & charts, etc.),
- This guidance extends as appropriate to the supply chains of all the above, which use or are involved in the delivery of hardware, software and information exchange; and
- Where appropriate, requirements relating to military aviation might also be in the scope of this document.

The military and its special role and position in the aviation system, its motivations, constraints and capabilities are fundamentally different when compared with the economic and safety focused approach of civil aviation because the primary objective for military aviation is to ensure security and defense of national airspace. Aside from this objective,

 © 2021 RTCA, Inc.