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

Information Security Guidance for Continued Airworthiness

RTCA DO-355A
September 10, 2020

Prepared by: SC-216

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

FOREWORD

This document was prepared by Special Committee 216 (SC-216) and EUROCAE Working Group 72 (WG-72). It was approved by the RTCA Program Management Committee (PMC) and by the EUROCAE Council on September 10, 2020.

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 Telecommunications 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.

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

TABLE OF FIGURES

1 INTRODUCTION

This document is a joint product of two industry committees: the EUROCAE Working Group WG-72, titled "Aeronautical Systems Security" and the RTCA Special Committee SC-216, also titled "Aeronautical Systems Security". WG-72 was formed to address information security and the overall Aeronautical Information System Security (AISS) of airborne systems in conjunction with related ground systems and environment, while SC-216 was formed more specifically to address information security for certification and operation of aircraft and its systems. The guidance provided by this document is intended to constitute an Acceptable Means of Compliance for approving information security aspects of Continuing Airworthiness activities performed by Design Approval Holders and Operators.

This document provides guidance for the operation and maintenance of aircraft and for organizations and personnel involved in these tasks. It is intended to support the responsibilities of the Design Approval Holder (DAH) to obtain a valid airworthiness certificate and aircraft operators to maintain their aircraft to demonstrate that the effects on the safety of the aircraft of information security threats are confined within acceptable levels. As all information security threats may have an intentional origin, this document also covers Intentional Unauthorized Electronic Interaction (IUEI).

1.1 Purpose

This document is a resource for civil aviation authorities and the aviation industry when the operation and maintenance of aircraft and the effects of information security threats can affect aircraft safety. It deals with the activities that need to be performed in operation and maintenance of the aircraft related to information security threats.

This document gives also guidance that is related to operational and commercial effects (i.e. guidance that exceeds the safety-only effects).

ED-204A / DO-355A is a companion document to ED-202A / DO-326A "Airworthiness Security Process Specification" and ED-203A / DO-356A "Airworthiness Security Methods and Considerations" that support security in the development and modification part of the airworthiness process.

Note 1: This document was developed in the European context of the European Aviation Safety Agency (EASA) Certification Specification CS-25 "Large Aeroplanes" and the United States context of Title 14 Code of Federal Regulations (14CFR) Part 25 "Transport Category Aircraft". Tailoring of this guidance may be used in other regulatory contexts including but not limited to CS-23, CS-27, CS-29, CS-E, CS-P, Part 23, Part 27, Part 29, Part 33, and Part 35.

The most comprehensive possible area of the application of this guidance is deemed to be Large Transport Aircraft programs. However, this document does not make any assumptions about and is without prejudice to its applicability.

Note 2: The measures proposed in this document may be subject to commercial terms between DAHs and operators. It is recommended that DAHs incorporate these elements into their commercial offers, especially for service and support related topics.