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

Guidance for Security Event Management

RTCA DO-392
June 23, 2023

Prepared by: SC-216

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 June 23, 2022.

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

TABLE OF FIGURES

TABLE OF TABLES

1 INTRODUCTION

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. The guidelines in this document were developed with the intent to provide Acceptable Means of Compliance to EASA's proposed Part IS which intends to establish a regulation requiring approved organizations to implement an Information Security Management System including (Security) Occurrence Reporting analogous to Safety Management System with (Safety) Occurrence Reporting. Other regulations may also apply. Organizations may elect to apply Information Security Event Management processes for operational or other business needs.

Information Security Event Management addresses security events with actual or potential safety consequences. Security events could be malicious interactions (hacking), non-targeted attacks (malware), as well as flaws (vulnerabilities) in systems components or procedures that could be exploited to cause safety consequences for the aircraft, its passengers or crew.

1.1 Purpose

This document is a resource for civil aviation authorities, government agencies (when applicable), and the aviation industry that need to address information security threats that can affect aviation safety. It addresses the management of security events that affect aviation safety and it supports the existing safety event management guidance. It provides guidance for detection, assessment and disposition, sharing information, reporting and other activities that need to be performed in response to information security events.

Aircraft manufacturers, operators, aviation service providers, maintenance repair and overhaul organizations (MRO), design, manufacturing, operation and regular maintenance of ground ATM/ANS equipment, industrial equipment manufacturing or supporting the production of aircraft and supporting systems and operators of information systems used for support of these functions and all other stakeholders of civil aviation can use this document for event management guidance.

This document is also intended to be a companion to other documents produced by EUROCAE WG-72 and RTCA SC-216 relating to Aeronautical Information System Security. This document is specifically intended for managing information security events that affect aviation safety but is also without prejudice as to its use in other contexts. It is intended to be used along with the safety event management processes defined by 14 CFR 21.3 (FAA), 14 CFR 135.415, 14 CFR 145.221 and Part 21.A.3A (EASA).

Regulatory agencies can publish additional guidance as well as point to existing industry standards, which may be used in combination with this document. Since aircraft information security requirements and regulations evolve, it is recommended that applicants monitor the applicable certification authority's guidance.

1.2 Scope

This document provides guidance to the aviation sector for the management of information security events with actual or potential aviation safety consequences. This includes unwanted or unexpected events that are an indication of an actual adverse effect on

