RTCA, Inc.
1828 L Street, NW, Suite 805
Washington, DC 20036-5133 USA

Integrated Security System Standard for Airport Access Control

RTCA DO-230C
Supersedes DO-230B
June 22, 2011

Prepared By: SC-224

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 the RTCA Special Committee 224 (SC-224) and approved by the RTCA Program Management Committee (PMC) on June 22, 2011.

RTCA, Inc. 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 Federal advisory committee 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, knowledge and practices in a manner that helps government and industry meet their mutual objectives and responsibilities.
- Analyzing and recommending solutions to 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.
- Assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization, 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.

The RTCA is not an official agency of the U.S. 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.

This Page Intentionally Left Blank

Document Background

The RTCA Special Committee 207 was assembled in 2005 when it became clear that the second version of DO-230 (Standards for Airport Security Access Control Systems) issued in 2003 was becoming obsolete.

This was due to the widespread introduction of smart cards and biometric technology in other areas, especially the Personal Identity Verification (PIV) initiative for Federal workers and the maritime Transportation Worker Identification Credential (TWIC) program. It had originally been intended to update the DO-230A document within a year of original issue. This proved not possible, and it was only by 2005 that a consensus for the requirement for an upgrade developed.

The standard DO-230B was re-issued in June 2008, with a significantly expanded increase in detail of the new areas of credentialing and biometrics.

Since then, the technical progress has continued and resulted in this document becoming obsolete (again). The cause of this was the yet again technical progress, the introduction of the PIV II and TWIC specifications, and the need to align the standard to the new version of the "Recommended Security Guidelines for Airport Planning, Design & Construction", issued by TSA in 2011.

This document had an accelerated implementation schedule and to remain compatible it was necessary to have an updated version of this RTCA standard by spring of 2011.

Accordingly, only an update addressing the above-mentioned changes was developed, recognizing that a full update would be required soon, probably commencing in early 2012.

Cooperation with TSA

Special Committee 224 has worked in close cooperation with the Transportation Security Administration (TSA) and their various credentialing efforts to ensure that this updated document contains the most current information regarding aviation credentialing initiatives.

This Page Intentionally Left Blank

EXECUTIVE SUMMARY

This document is an update to RTCA DO-230B, "Standards for Airport Security Access Control Systems," published in 2008.

It provides standards and guidelines for implementing access control systems in the context of an Integrated Security System for an airport. The document provides guidance on acquiring and designing such systems, testing and evaluating system performance, and operational requirements.

It should be emphasized that these guidelines and standards are not regulatory in nature, but represent the industry's derived consensus on standards and provisions to be met in achieving consistency and interoperability in an airport access control environment.

This updated document incorporates the latest technological advances in security access control systems and identity management technologies, including smart cards and biometrics. The nature of the changes in available technology, and the need to include perimeter security, security operation support and identity management requirements, has led to a major change in the layout and content of the document. The major areas covered are:

- System level requirements.
- Identity management requirements.
- Physical access control requirements.
- Intrusion detection requirements.
- Video surveillance requirements.
- Security operating center requirements.
- Communications infrastructure requirements.
- General procurement level guidance.

The document also contains numerous appendices that provide minimum performance guidance and reference material on several areas including standards, magnetic stripe track use, glossary and references.

This document is not a complete revision of the previous version, but just an update. The cause of this was yet again technical progress, the introduction of the PIV-I and -C specifications, and the need to align the standard to the new version of the "Recommended Security Guidelines for Airport Planning, Design & Construction" issued by the TSA in 2011.

This document had an accelerated implementation schedule and to remain compatible it was necessary to have an updated version of this RTCA standard by spring of 2011.

Accordingly, only an update addressing the above mentioned changes was developed, recognizing that a full update would be required soon, probably commencing in early 2012.

A list of the areas which were identified by the committee for update in the next version of DO- 230 is included in the introduction section.

Following the approach adopted in DO-230B, and recognizing that both technology and regulation proceed apace and await no man, it was decided that a strict adherence to what was required by the regulations at the date of issue was pointless as it would be quickly obsolete.

As a result, the document indicates not only the current best practices and system requirements to meet the current regulatory requirements, but also provides guidance for those airports who wish to go beyond these requirements, and provides guidance for what the committee believes are logical and reasonable methods for implementing the advances in security technology.

In this regard, the committee has received substantial input from the TSA and this has resulted in several forward-looking sections, specifically in the identity management and physical access credential areas.

The information contained herein represents the experience of airports and their professional associations (American Association of Airport Executives and Airports Council International-North America); the Airport Consultants Council; the security technology industry (i.e., standards organizations, industry organizations, vendors, integrators); airlines, and their associations (Air Transport Association); and airport-regulating federal agencies (the FAA and the TSA).

This document was prepared by RTCA Special Committee (SC) 224, which included in its membership representatives from all of the above groups and agencies, as well as representatives from the interested public.

TABLE OF CONTENTS

This Page Intentionally Left Blank

1 INTRODUCTION

1.1 Purpose

This document contains standards and guidelines for Airport Security Access Control Systems, and supporting systems, (including alarm monitoring, credentialing, identity management, biometrics, video management and recording, intrusion detection, intercom, public address, and supporting network communications subsystems) hereinafter called Integrated Security System for Airports, (ISSA), including guidance in the application of biometrics and identity management and credentialing.

Airports designing or enhancing such systems under the Code of Federal Regulations (CFR), Title 49 (Transportation Security Administration [TSA]), Part 1542.207, are strongly encouraged to consider these recommendations in the design and implementation process.

These standards present functional requirements and performance characteristics, and best practices for use by designers, manufacturers, installers, service providers, operators and users of automated ISSA intended for operational use within the U.S. National Airspace System (NAS) and include industry best practices and lessons learned by industry subject matter experts.

1.2 History

In 1973, the Federal Aviation Administration (FAA) divided responsibility for aviation security between the airlines and the airport operators.

Airlines were required to screen passengers and the airport operators were required to have an FAA-approved Airport Security Program (ASP). FAR Part 107 was promulgated to provide a secure environment in which airlines could operate.

This ASP must describe the functions and procedures to control access to secured areas of the airport and control movement of persons and vehicles within those areas. The personnel identification and challenge procedures contained in ASPs provide an additional layer of security once an individual has gained access to a restricted area. However, these procedures could still allow an individual using forged, stolen or non-current identification to compromise the secured area. Former employees could also use their familiarity with airline and airport procedures to attempt to enter a secured area.

The FAA issued, on January 6, 1989, a new section, FAR 107.14, to Part 107 to address these concerns. The regulation provided for the installation and use of a system, method or procedure that meets certain performance standards to prevent unauthorized access to secured areas of airports. Although the performance standards were developed with automated Physical Access Control Systems (PACS) in mind (FAR 107.14[a]), they do allow the installation and use of systems, methods or procedures other than computer-controlled access.

The final rule further added paragraph FAR 107.14(b) that provided for FAA approval of alternative systems, methods or procedures that provide an overall level of security equal to that established by the performance standards in FAR 107.14(a).

Airport operators were required to segregate the secured area from other areas of the Air Operations Area (AOA) so that (1) access controls that meet the requirements of FAR 107.14 were used to protect the area where commercial passenger aircraft are accessible and (2) procedures to control the movement of persons and vehicles that meet the requirements of FAR 107.13 were used for other portions of the AOA.