RTCA, Incorporated
1828 L Street, NW, Suite 805
Washington, DC 20036

STANDARDS FOR AIRPORT SECURITY ACCESS CONTROL SYSTEMS

RTCA DO-230A
Supersedes DO-230
April 10, 2003

Prepared by SC-199

Copies of this document can be obtained from

RTCA, Incorporated
1828 L Street, NW, Suite 80[illegible]
Washington, DC 20036 USA

Telephone: 202-83[illegible]9329
Facsimile: 202-833-9434

www.rtca.org

Please call RTCA for price and ordering information.

FORWARD

This report was prepared by the RTCA Special Committee 199 and approved by the RTCA Program Management Committee (PMC) on April 10, 2003.

The 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 Federal Advisory Committee and develops consensus-based recommendations on contemporary aviation issues. The 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 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.

Since 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.

Document Background

Unlike many other RTCA documents, which typically have a five-year or more "life", the subject of this document is in a very fluid regulatory and technical environment. The committee recognized this and expects an update will be required within 1-2 years. The committee accepted the urgent need to provide up to date guidance to airports and rejected the option of waiting until the situation was more stable.

The RTCA SC199 was assembled prior to the tragic events of September 11, 2001, with the intent to provide an update to the existing document (DO-230). However, with the establishment of the Transportation Security Administration (TSA) and other additional security requirements in the Aviation and Transportation Security Act (ATSA), November 11, 2001, its deliberations were extended to cover the new requirements and access control technology developments. Thus, there are significant sections in this document on smart cards and biometrics and other relevant security measures mentioned in the ATSA. With regard to the technology airport pilot test programs, it is expected that these will include biometric testing. Accordingly, the section of biometrics is provisional awaiting the results of those tests in an operational environment. It would be appropriate to reconvene the committee within 1 year from the issuance of this document so the document can be updated to reflect the findings of these pilot test programs and address other potential changes in the ATSA.

The SC199 has worked in close cooperation with the TSA and their various credentialing efforts. It will continue this close cooperation to ensure that at the next rewrite contains the most current information regarding aviation credentialing efforts.

EXECUTIVE SUMMARY

This document is a release of the updates to RTCA DO-230, *Standards for Airport Security Access Control Systems (ACS)*, originally published in 1996, updated with information current as of December 31, 2002. It provides minimum performance standards and guidelines for access control systems (ACSs) in airports. The document provides guidance on acquiring and designing an ACS, testing and evaluating system performance, and operational requirements. It should be emphasized that these guidelines and performance standards are not regulatory in nature, but represent the industry's derived consensus on minimum performance standards to be met in achieving consistency and interoperability in an airport access control environment.

This updated document incorporates the latest technological advances in ACSs technologies, addressing smart cards and biometrics. Since the original DO-230 release, there have been major developments in the access control technologies used and evolving standards to ensure robust system architecture and common subsystem communications platforms and interfaces. Rapid advances in the fields of biometrics and chip technology have necessitated the need to include detailed guidance in these areas, as provided in Appendix A.

This document also provides guidance on networking ACSs, the use of wireless technology, and updates to 49 Code of Federal Regulations (CFR), Part 1542 (Airport Security), which replaces guidance based on the superseded Federal Aviation Regulation (FAR) 107/108 from the original document.

Using the original DO-230 format, this document has been expanded in the following sections:

- Section 1 introduces the ACS, purpose, scope, goals, and operational requirements.
- Section 2 provides guidance for system performance.
- Section 3 addresses subsystem performance of access media and hardware.
- Section 4 provides guidance for system verification and validation.

The document also contains the following three appendixes that provide minimum performance guidance and reference material:

- Appendix A provides detailed guidance on biometrics and smart card technologies.
- Appendix B provides reference examples of sample reports commonly found in ACSs.
- Appendix C is a list of acronyms and abbreviations used in this document.

The information contained herein represents 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., ACS vendors, integrators); airlines, pilots and their associations (Air Transport Association and Air Line Pilots Association, respectively); and airport regulating federal agencies (the FAA and the TSA). This document was prepared by RTCA Special Committee 199, which included in its membership representatives from all of the above groups and agencies, as well as representatives from the interested public.

This page intentionally left blank.

TABLE OF CONTENTS

APPENDIXES

TABLE OF TABLES

TABLE OF FIGURES

1 INTRODUCTION

1.1 Purpose and Scope

This document contains recommended minimum performance standards and guidelines for Airport Security Access Control Systems (ACSs), including guidance in the application of biometrics. Airports designing or enhancing ACSs 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 process.

These standards present functional requirements and performance characteristics for use by designers, manufacturers, service providers, operators and users of automated ACSs intended for operational use within the U.S. National Airspace System (NAS).

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.

For FAA/TSA approval, ASPs 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 a means of control 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 ACSs 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 provides 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 should 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 are 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 are used for other portions of the AOA.

In July 2001, a new version of the FAR 107 was issued, with minor changes without significant impact on ACS design. The relevant section was renamed to FAR 207.