RTCA, Inc.
1150 18th Street, NW, Suite 910
Washington D.C. 20036

Standards for Airport Security Access Control Systems

RTCA DO-230D
December 18, 2013

Prepared by SC-224

FOREWORD

This report was prepared by RTCA Special Committee 224 (SC-224) and approved by the RTCA Program Management Committee (PMC) on December 18, 2013.

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. 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 several 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.

This Page Intentionally Left Blank

EXECUTIVE SUMMARY

This document is a full revision to RTCA *DO-230C, Standards for Airport Security Access Control Systems, (2011)* providing standards and guidelines for implementing access control systems in the context of integrated security systems for airports. 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 enhance sections pertaining to 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:

- Introduction and Overview
- Credentialing
- Biometrics
- Physical Access Control Systems (PACS)
- Perimeter Intrusion Detection Systems (PIDS)
- Video Surveillance Systems
- Security Operations Center (SOC)
- Integration
- Communications Infrastructure
- General Acquisition-Related Considerations

Following the approach adopted in previous versions of *DO-230*, 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 airport operators who wish to go beyond these requirements and forward what the Committee believes are logical and reasonable methods for implementing the advances in security technology.

In this regard, Special Committee 224 has received input from the TSA and this has resulted in several forward-looking statements and inputs from the TSA *Recommended Security Guidelines for Airport Planning, Design and Construction, (May 2011)*. It should also be noted that although the TSA guidelines cover passenger screening areas and checkpoint security, those areas are outside the scope of this *DO-230* document. Section inputs from airport operators and vendors relied on actual experience and operational issues faced while implementing access control systems and several lessons learned were included as guidance for future consideration by system developers.

Privacy concerns have been raised as they relate to video surveillance using closed circuit television systems (CCTV), cameras used in perimeter intrusion detection systems (PIDS), and the use of drones / unmanned aerial vehicles (UAV). These paradigm shifts in the use of advanced imaging technology have resulted in the need to address privacy and protect the images captured by these systems and information sharing by airport stakeholders at all levels. While the *FAA Reauthorization Act of 2012* requires the FAA to address the issue of drones / UAVs, that agency's primary mission is safety rather than security; thus, safety-related actions in this area have been deemed to be outside the scope of this document.

Some captured images may be federally classified as *Security Sensitive Information* (SSI) thus restricting their distribution and/or public release. Airport security plans and programs should include risk mitigations as to privacy in operational and procedural scenarios and ensure security controls are adequate in controlling who has access to information and how it may be shared. The Department of Homeland Security (DHS) has established a Privacy Office and its *Privacy Incident Handling Guidance, January, 2012* is available for reference on its website.

The RTCA *DO230D* document contains forward-thinking references to technology, processes and guidance as continue to evolve. Where applicable, the Committee has made these references in the interest of providing a complete picture of the possible direction of a standard and/or technology. An example of this is the evolution of cloud computing and the ongoing development of standards by various professional, academic and standards organizations. The (US) Government Accountability Office (GAO) issued a report on future cloud computing efforts and the need for better planning (*GAO-12-756: Information Technology Reform – Progress Made but Future Cloud Computing Efforts Should be Better Planned*). RTCA Special Committee (SC) 224 recommends that readers of this guidance document solicit the latest information on any referenced technology, processes and procedures before moving forward with planned implementation of an airport security access control system. Finally, this document provides information on technology trends in physical access control systems (PACS), access card technology, video, wireless and physical security information management systems (PSIM) that are deemed current at the time of publication, but may be obsolete or overcome by other emerging technology. Airport operators are reminded that this information provides current guidance to support well-informed appropriate decision-making in addressing particular facilities.

Further, the information contained herein represents the experience of airport operators and their professional (American Association of Airport Executives (AAAE), Airport Consultants Council (ACC)) and industry (Airports Council International-North America (ACI-NA) associations, as well as security technology industry (i.e., standards organizations, industry organizations, vendors, integrators); airline industry bodies such as International Air Transport Association (IATA) and Airlines for America (A4A) as well as aviation / airport regulatory bodies such as FAA and 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. The reader should be aware that sections of the document were created by separate groups of subject matter experts in their respective fields resulting in different styles and structure. These nuances should in no way detract from the substance of the subject matter contained within the individual chapters.

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Purpose

This document contains standards and guidelines for airport security access control and integrated systems (including alarm monitoring, credentialing, identity management, biometrics, video management and recording, intrusion detection, intercom, public address, and supporting network communications subsystems) and is hereinafter entitled *Integrated Security Systems for Airports* (ISSA).

Airport operators designing or enhancing such systems under the *Code of Federal Regulations (CFR), Title 49 (Transportation Security Administration [TSA]), Chapter XII, 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 integrated security systems 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). Federal Aviation Regulation *(FAR) Part 107* was promulgated to provide a more secure environment in which airlines could operate.

Airport operations vary from place and place. Each ASP was originally required to describe the means and procedures in place to control personnel and vehicle access to and within secured areas. ASP personnel identification and challenge procedures, for instance, enhanced the security inherent in the use of airport-issued employee identity badges mitigating the possible use of forged, stolen or non-current identification by no-longer-authorized individuals seeking to exploit this knowledge in attempting to enter secured areas.

With the FAA issuance of *FAR 107.14 (1989)*, the installation and use of systems, equipment, and other means of meeting certain performance standards to prevent unauthorized access to secured areas of airports was strengthened. 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 in *FAR 107.14(b)* 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) to ensure (1) access controls specifically restrict access to commercial passenger aircraft areas and (2) controlled vehicle and personnel movements in other portions of the AOA as required by *FAR 107.13.* In July 2001, an entirely new version of the *FAR 107* was issued, with largely procedural changes, but without significant impact on Physical Access Control System (PACS) design.

Subsequent to the transfer of the security responsibility to the TSA as required by the *Aviation Transportation Security Act (ATSA) November 2001*, these regulations were relocated, with few significant changes, to *CFR, Title 49*, Chapter XII, *Parts 1500-1699.* In *1542.207,* the division of responsibility between the airlines, airport and federal agencies was modified by ATSA. However, while