

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

Integrated Security System Standard for Airport Access Control

RTCA DO-230B
Supersedes DO-230A
June 19, 2008

Prepared by: SC-207
© 2008 RTCA, Inc.

Copies of this document may be obtained from:

RTCA, Inc.

Telephone: 202-833-9333

Facsimile: 202-833-9433

Internet: www.rca.org

Please visit the RTCA Online Store for document pricing and ordering information.

FOREWORD

This report was prepared by the RTCA Special Committee 207 and approved by the RTCA Program Management Committee (PMC) on June 19, 2008.

The RTCA 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, knowledge and practice 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.

Document Background

The RTCA SC-207 committee 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.

Since then, the progress made in other areas of access control and identity management has continued apace, and this has extended the duration of the committee deliberations beyond the scheduled delivery date.

Cooperation with TSA

The SC-207 Committee has worked in close cooperation with the Transportation Security Administration (TSA) and their various credentialing efforts, including the TSA Transportation Threat Assessment and Credentialing (TTAC) office, to ensure that this updated document contains the most current information regarding aviation credentialing initiatives.

Currently in preview, click buy full versi

EXECUTIVE SUMMARY

This document is an update to RTCA DO-230A, "Standards for Airport Security Access Control Systems," originally published in 2003.

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 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.

It should also be noted that the information included in this standard is different in nature from that provided in the previous issue(s). Recognizing that both technology and regulation proceed apace and afield, 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 what are 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) 207, 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

1	<u>INTRODUCTION</u>	2
1.1	PURPOSE	2
1.2	HISTORY	2
1.3	SCOPE	3
1.4	SYSTEM OVERVIEW	4
1.5	OPERATIONAL GOALS	5
1.6	ACRONYMS AND DEFINITION OF TERMS	5
2	<u>REQUIREMENTS AND SYSTEM DESIGN</u>	7
2.1	REGULATORY REQUIREMENTS	7
2.1.1	TSA AVIATION CREDENTIAL INTEROPERABILITY SOLUTION	7
2.2	INTEGRATED SECURITY SYSTEMS FOR AIRPORTS (ISSA)	8
2.2.1	THREATS, VULNERABILITIES, AND RISKS	9
2.2.2	REQUIREMENTS PROCESS	12
2.2.3	INFORMATION FOR MANAGING SECURITY OPERATION	14
2.3	ISSA SYSTEM ENGINEERING	15
2.3.1	SYSTEM CONCEPT	16
2.3.2	THE SECURITY OPERATIONS CENTER (SOC)	18
2.3.3	NETWORKED COMMUNICATIONS INFRASTRUCTURE	18
2.3.4	PHYSICAL ACCESS CONTROL SYSTEM (PACS)	18
2.3.5	IDENTITY MANAGEMENT AND CREDENTIALING	19
2.3.6	INTRUSION DETECTION SYSTEM (IDS)	21
2.3.7	VIDEO SURVEILLANCE AND MANAGEMENT SYSTEM	22
2.4	EXECUTING THE SYSTEM DESIGN	23
2.4.1	STANDARDS-BASED OPEN ARCHITECTURE	23
2.4.2	SYSTEM AND APPLICATION SOFTWARE	24
2.4.3	SYSTEM COMPONENT INTEROPERABILITY	24
2.4.4	MODULARITY	25
2.4.5	SCALABILITY	25
2.4.6	RELIABILITY, MAINTAINABILITY, AND AVAILABILITY	25
2.4.7	SYSTEM CAPACITY AND THROUGHPUT	26
2.4.8	DATA MANAGEMENT	27
2.4.9	ACQUISITION STRATEGY AND ISSUES	27
2.4.10	INSTALLATION, TRAINING, AND MAINTENANCE	28
2.5	INTEGRATED SECURITY SYSTEM FOR AIRPORTS (ISSA) DESIGN CHECKLIST	29
3	<u>IDENTITY MANAGEMENT AND CREDENTIAL ISSUANCE</u>	33
3.1	INTRODUCTION	33
3.1.1	IDENTITY RELATED VULNERABILITY OR WEAKNESSES	34
3.1.2	ONCE AND FUTURE STATE	36
3.2	DEFINITIONS	36
3.2.1	FOUNDATIONAL DEFINITIONS	36

3.2.2	PERSON/HUMAN ORIENTED DEFINITIONS	37
3.2.3	MORE ABOUT “CREDENTIAL” - A COMPREHENSIVE VIEW WITH DEFINITIONS	38
3.3	IDENTITY MANAGEMENT AND CREDENTIAL ISSUANCE SYSTEM (IDM-CIS) TAXONOMY	40
3.3.1	OUTLINE VIEW OF THE FUNCTIONS AND COMPONENTS OF AN IDM-CIS	40
3.3.2	FUNCTIONAL VIEW OF THE IDM-CIS AND ITS INTERCONNECTIONS	44
3.3.3	COMPONENT VIEWS OF THE IDM-CIS AND ITS INTERCONNECTIONS	44
3.4	IDENTITY MANAGEMENT AND CREDENTIAL ISSUANCE SYSTEM CONCEPTS	52
3.4.1	ENABLING TECHNOLOGIES	52
3.4.2	CHAIN OF TRUST	52
3.4.3	IDM-CIS WORKFLOW	55
3.4.4	ENROLLMENT CONSIDERATIONS	54
3.4.5	IDMS GENERIC DATABASE	54
3.4.6	THREAT/RISK AND SUITABILITY	58
3.4.7	POST ISSUANCE CREDENTIAL MAINTENANCE	59
3.4.8	FIPS 201 PERSPECTIVE ON IDM-CIS CONCEPTS	61
3.5	IDM-CIS COMPONENT DETAILED DESCRIPTIONS	63
3.5.1	ENROLLMENT STATION	63
3.5.2	ID MANAGEMENT COMPONENTS	64
3.5.3	CARD PRODUCTION FACILITY	69
3.5.4	ISSUANCE STATION	70
3.6	MIGRATION STRATEGIES FOR IDENTITY CREDENTIALS	72
ANNEX 3 SECTION THREE ANNEXES		77
<hr/>		
A-3.1	IDENTITY MANAGEMENT	77
A-3.2	CREDENTIALS	82
4 PHYSICAL ACCESS CONTROL SYSTEMS, PACS		107
<hr/>		
4.1	OVERVIEW	107
4.2	MAJOR COMPONENTS	108
4.2.1	GENERAL WORKFLOW	108
4.2.2	SECURITY BOUNDARY	109
4.2.3	REGISTERING PHYSICAL ACCESS PRIVILEGES	111
4.2.4	EXTERNAL IT INTERACTIONS	111
4.3	MIGRATION	112
4.4	PACS INTEGRATION INTO INTRUSION DETECTION SYSTEM	112
4.5	CARD (CREDENTIALS)	114
4.6	PORTAL HARDWARE	114
4.6.1	READERS	115
4.6.2	SMART CARD READER AND DATA FORMATS	117
4.7	PACS FIELD CONTROLLER	117
4.8	PACS SERVER HARDWARE	120
4.8.1	OS SELECTION, CONFIGURATION AND SIZING	121
4.8.2	AVAILABILITY, REDUNDANCY AND RAID	122
4.9	SOFTWARE	123
4.9.1	SOFTWARE CHARACTERISTICS	123
4.10	DATABASE DESIGN AND MANAGEMENT	124
4.10.1	DATABASE DESIGN CONSIDERATIONS	126
4.10.2	CENTRALIZED DATABASE PACS	127

4.10.3	DISTRIBUTED DATABASE PACS	127
4.11	CLIENT WORKSTATIONS	128
4.12	SECURITY CERTIFICATION AND ACCREDITATION	128
ANNEX 4 SECTION FOUR ANNEXES		129
<hr/>		
ANNEX 4.1	BIOMETRICS IN PHYSICAL ACCESS CONTROL SYSTEMS	129
ANNEX 4.2	LOCKING HARDWARE BARRIERS, ETC IN PACS	138
5 INTRUSION DETECTION SYSTEMS		144
<hr/>		
5.1	INTRODUCTION	144
5.2	INTRUSION DETECTION AND TRACKING	145
5.2.1	INTRUDER CHARACTERISTICS	145
5.2.2	INTRUDER DETECTION	146
5.2.3	ALARM GENERATION	146
5.2.4	INTRUDER CLASSIFICATION	146
5.2.5	INTRUDER TRACKING	146
5.2.6	PERFORMANCE MEASURES	147
5.3	SECURITY FORCE TRACKING	148
5.4	INTRUSION ASSESSMENT AND SURVEILLANCE	148
5.4.1	CAMERA CHARACTERISTICS	148
5.4.2	CAMERA CONTROL	149
5.4.3	INTRUSION ASSESSMENT	149
5.4.4	PERFORMANCE MEASURES	149
5.5	LIGHTING REQUIREMENTS	149
5.6	INTRUSION DETECTION AND TRACKING TECHNOLOGIES	150
5.6.1	VIDEO MOTION DETECTION	151
5.6.2	VIDEO-BASED TRACKING	152
5.6.3	RADAR SYSTEMS	152
5.6.4	LADAR SYSTEMS	155
5.6.5	ACTIVE INFRARED (EXTERIOR)	156
5.6.6	ACTIVE INFRARED (INTERIOR)	156
5.6.7	PASSIVE INFRARED (INTERIOR)	157
5.6.8	FENCE VIBRATION	157
5.6.9	FIBER-OPTIC CABLE	157
5.6.10	UNDERWATER FIBER-OPTIC NETTING	158
5.6.11	BURIED PRESSURE LINE SENSOR	158
5.6.12	PORTED COAX BURIED CABLE	158
5.6.13	TAUT WIRE	159
5.6.14	BI-STATIC MICROWAVE	159
5.6.15	OTHER TECHNOLOGIES	160
5.7	REFERENCE DOCUMENTS	160
6 VIDEO SURVEILLANCE		163
<hr/>		
6.1	VIDEO SURVEILLANCE AND VIDEO MANAGEMENT	163
6.1.1	VIDEO IMAGING SENSORS	163
6.1.2	APPLICATIONS	167

6.2	VIDEO PERFORMANCE REQUIREMENTS	170
6.3	LIGHTING	171
6.4	VIDEO MANAGEMENT	174
6.4.1	EDGE ARCHITECTURE, TRANSMISSION BANDWIDTH, AND DIGITAL VIDEO STORAGE	175
6.4.2	VIDEO ANALYTICS	176
6.4.3	DIGITAL VIDEO RECORDING - RAID, NAS, AND SAN	179
6.4.4	VIDEO SERVERS	181
7	<u>SECURITY OPERATIONS CENTER (SOC)</u>	<u>184</u>
7.1	INTRODUCTION	184
7.2	FACILITIES: STANDARD SECURITY OPERATIONS CENTER	185
7.2.1	FACILITIES: STANDARD SOC DESIGN / BUILD / OPERATION CONSIDERATIONS	186
7.2.2	FACILITIES: SOC SUPPORTING PACS COMMUNICATIONS INFRASTRUCTURE	186
7.3	FUNCTION: SECURITY OPERATIONS CENTER (SOC) REQUIREMENTS	187
7.4	PHILOSOPHY: SOC AND SITUATIONAL AWARENESS	187
7.4.1	PHILOSOPHY: CONTINUING DOMAIN AWARENESS IN THE SOC	188
8	<u>COMMUNICATIONS INFRASTRUCTURE</u>	<u>191</u>
8.1	ESTABLISHING A COMMUNICATIONS INFRASTRUCTURE	191
8.2	COMMUNICATION INFRASTRUCTURE RELATIONSHIPS	192
8.2.1	COMMUNICATIONS INFRASTRUCTURE FUNCTIONALITY	193
8.3	COMMUNICATIONS CHARACTERISTICS	195
8.4	NETWORK DESIGN	196
8.4.1	DESIGN OBJECTIVES	196
8.4.2	LAN PROTOCOLS	197
8.4.3	OSI MODEL	198
8.4.4	TOPOLOGIES	199
8.4.5	VLANs	201
8.4.6	BANDWIDTH MANAGEMENT	201
8.4.7	QUALITY OF SERVICE (QoS) ISSUES	202
8.4.8	IP VOICE	203
8.4.9	MULTICASTING	203
8.4.10	VPN	204
8.4.11	WIRELESS COMMUNICATIONS	204
8.4.12	NETWORK SECURITY	209
8.5	PHYSICAL CABLE PLANT	211
8.5.1	CABLE PLANT MIGRATION STRATEGY	212
8.5.2	WIRE AND CABLE INSTALLATION	212
8.6	PHYSICAL PROTECTION OF NETWORK ASSETS	213
9	<u>GENERAL ACQUISITION RELATED CONSIDERATIONS</u>	<u>216</u>
9.1	INTRODUCTION	216
9.2	REGULATORY REQUIREMENTS	216
9.2.1	FEDERAL, STATE, AND LOCAL REGULATORY REQUIREMENTS	216
9.3	SYSTEM ACQUISITION PHASE	218

9.3.1	SYSTEM DESIGN	218
9.3.2	SYSTEM DESIGN OBJECTIVES	219
9.3.3	LEGACY SYSTEM INTEGRATION	220
9.3.4	SYSTEM SPECIFICATION AND SELECTION	221
9.4	SYSTEM INSTALLATION PHASE	222
9.5	IMPLEMENTATION PHASING CONSIDERATIONS	222
9.6	SYSTEM DOCUMENTATION	223
9.6.1	AS BUILT DRAWINGS AND LIST OF MATERIALS	223
9.6.2	OPERATIONAL PROCEDURES FORMAT AND CONTENT	223
9.7	TRAINING MANUALS AND COURSES	223
9.7.1	ISSA OPERATOR TRAINING	224
9.7.2	SYSTEMS ADMINISTRATOR TRAINING	224
9.7.3	MAINTENANCE TRAINING	224
9.7.4	BIOMETRICS – SPECIAL USER TRAINING CONSIDERATIONS	225
9.8	SYSTEM TEST, VERIFICATION AND VALIDATION	225
9.8.1	SYSTEM TEST	226
9.8.2	SPECIAL BIOMETRIC SUBSYSTEM TESTING AND CERTIFICATION	230
9.9	WARRANTY REQUIREMENTS	230
9.10	SYSTEM LOGISTICS SUPPORT	230
9.10.1	MAINTENANCE CONSIDERATIONS	231
<u>ANNEX 9 SECTION NINE ANNEXES</u>		<u>233</u>
A-9.1	REGULATIONS, CODES, STANDARDS AND GUIDELINES	233
A-9.2	OPERATIONAL AVAILABILITY, RELIABILITY, AND MAINTAINABILITY	237
A-9.3	FINAL AS-BUILT DRAWINGS AND LIST OF MATERIALS (LOM)	242
A-9.4	SAMPLE TEST PLAN (PACS ORIENTED)	245
<u>10</u>	<u>MEMBERSHIP</u>	<u>248</u>
<u>APPENDIX I STANDARDS</u>		<u>252</u>
I.1	IDENTIFICATION CARD TECHNOLOGY STANDARDS (MAGNETIC STRIPE AND SMART CARD)	253
I.2	PRINTED SURFACE FEATURES	254
I.2.1	PHOTOS	254
I.2.2	BARCODES	254
I.2.3	OPTICAL MEMORY	255
I.3	CONTACT INTERFACES	255
I.4	CONTACTLESS INTERFACES	258
I.4.1	COUNTRY-SPECIFIC ISSUES FOR CONTACTLESS	259
I.5	SECURITY AND ASSURANCE STANDARDS	259
I.6	IDENTITY DOCUMENT STANDARDS	260
I.7	BIOMETRIC STANDARDS	261
I.7.1	BIOMETRIC APPLICATION INTERFACE STANDARDS	261
I.7.2	BIOMETRIC APPLICATION PROFILE STANDARDS	263
<u>APPENDIX II MAGNETIC STRIPE TRACK USE</u>		<u>264</u>
II.1	FINANCIAL CARDS	264

II.2 DRIVER'S LICENSES (USA)	266
II.3 SEIWG-012 PHYSICAL ACCESS CONTROL (DOD)	267
II.4 FEDERAL AGENCY SMART CREDENTIAL NUMBER (GSC-IAB)	267
<u>APPENDIX III GLOSSARY</u>	<u>271</u>
<u>APPENDIX IV REFERENCES</u>	<u>282</u>
<u>V.1 ID SECURITY DEVICE ATTACHMENT</u>	<u>287</u>
V.2 THREAT LEVELS	288
V.3 THREAT TYPES	288
V.4 PRINTING	288
V.5 INKS	289
V.6 SUBSTRATE INCLUSION	290
V.7 OPTICALLY VARIABLE DEVICES (OVD)	291
V.8 ADDITIONAL FEATURES	292

1	INTRODUCTION	2
1.1	PURPOSE	2
1.2	HISTORY	2
1.3	SCOPE	3
1.4	SYSTEM OVERVIEW	4
1.5	OPERATIONAL GOALS	5
1.6	ACRONYMS AND DEFINITION OF TERMS	5

1 INTRODUCTION

1.1 Purpose

This document contains standards and guidelines for Airport Security Access Control Systems, and supporting systems, 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 for use by designers, manufacturers, service providers, operators and users of automated ISSA intended for operational use within the U.S. National Airspace System (NAS).

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 Access Control Systems (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 were required to segregate the secured area from other areas of the Air Operations Area (AOA) so that (1) access controls that meet the