

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
© 2011 RTCA, Inc.

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-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 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

1 INTRODUCTION.....	1
1.1 PURPOSE.....	1
1.2 HISTORY	1
1.3 SCOPE	2
1.4 SYSTEM OVERVIEW.....	2
1.5 OPERATIONAL GOALS.....	4
1.6 UPDATES POSTPONED TO NEXT VERSION	4
2 REQUIREMENTS AND SYSTEM DESIGN	5
2.1 REGULATORY REQUIREMENTS	5
2.1.1 TSA PARTICIPATION IN STANDARDS DEVELOPMENT.....	5
2.2 INTEGRATED SECURITY SYSTEMS FOR AIRPORTS (ISSA).....	5
2.2.1 THREATS, VULNERABILITIES, AND RISKS	5
2.2.2 REQUIREMENTS PROCESS	8
2.2.3 INFORMATION FOR MANAGING SECURITY OPERATION.....	10
2.3 ISSA SYSTEM ENGINEERING	11
2.3.1 SYSTEM CONCEPT	12
2.3.2 THE SECURITY OPERATIONS CENTER (SOC).....	14
2.3.3 NETWORKED COMMUNICATIONS INFRASTRUCTURE.....	14
2.3.4 PHYSICAL ACCESS CONTROL SYSTEM (PACS)	14
2.3.5 IDENTITY MANAGEMENT AND CREDENTIALING.....	15
2.3.6 INTRUSION DETECTION SYSTEM (IDS)	17
2.3.7 VIDEO SURVEILLANCE AND MANAGEMENT SYSTEM.....	18
2.4 EXECUTING THE SYSTEM DESIGN	19
2.4.1 STANDARDS-BASED OPEN ARCHITECTURE	19
2.4.2 SYSTEM AND APPLICATION SOFTWARE.....	19
2.4.3 SYSTEM COMPONENT INTEROPERABILITY.....	20
2.4.4 MODULARITY	20
2.4.5 SCALABILITY.....	21
2.4.6 RELIABILITY, MAINTAINABILITY, AND AVAILABILITY	21
2.4.7 SYSTEM CAPACITY AND THROUGHPUT	22
2.4.8 DATA MANAGEMENT	23
2.4.9 ACQUISITION STRATEGY AND ISSUES.....	23
2.4.10 INSTALLATION, TRAINING, AND MAINTENANCE	24
2.5 INTEGRATED SECURITY SYSTEM FOR AIRPORTS (ISSA) DESIGN CHECKLIST.....	25
3 IDENTITY MANAGEMENT AND CREDENTIAL ISSUANCE	27
3.1 INTRODUCTION	27
3.1.1 IDENTITY RELATED VULNERABILITY OR WEAKNESSES.....	28
3.1.2 ONCE AND FUTURE STATE	28
3.2 DEFINITIONS	31
3.2.1 FOUNDATIONAL DEFINITIONS.....	31
3.2.2 PERSON/HUMAN ORIENTED DEFINITIONS	32
3.2.3 MORE ABOUT “CREDENTIAL” - A COMPREHENSIVE VIEW WITH DEFINITIONS.....	33
3.2.4 ENABLING TECHNOLOGIES	35
3.2.5 CHAIN OF TRUST	35
3.2.6 FIPS 201 PERSPECTIVE ON IdM-CIS CONCEPTS	36
3.3 IDENTITY MANAGEMENT AND CREDENTIAL ISSUANCE SYSTEM TAXONOMY.....	37

3.3.1	OUTLINE VIEW OF THE FUNCTIONS AND COMPONENTS OF AN IDM-CIS	37
3.3.2	FUNCTIONAL VIEW OF THE IDM-CIS AND ITS INTERCONNECTIONS	40
3.4	IDENTITY MANAGEMENT AND CREDENTIAL ISSUANCE SYSTEM CONSIDERATIONS.....	42
3.4.1	IDM-CIS DEPLOYMENT CONSIDERATIONS	42
3.4.2	IDM-CIS ARCHITECTURAL CONSIDERATIONS.....	43
3.4.3	ENROLLMENT CONSIDERATIONS	47
3.4.4	IDMS GENERIC DATABASE CONSIDERATIONS.....	47
3.4.5	BIOMETRIC TRAINING AT ISSUANCE.....	51
3.4.6	THREAT/RISK AND SUITABILITY CONSIDERATIONS.....	52
3.4.7	POST ISSUANCE CREDENTIAL MAINTENANCE CONSIDERATIONS	52
3.5	MIGRATION STRATEGIES FOR IDENTITY CREDENTIALS	55
ANNEX 3 SECTION THREE ANEXES		61
A-3.1	IDM-CIS COMPONENT DETAILED DESCRIPTIONS.....	61
A-3.1.1	ENROLLMENT STATION	61
A-3.1.2	IDMS.....	61
A-3.1.2.1	WORKFLOW MANAGER.....	62
A-3.1.2.2	WEB PORTAL.....	62
A-3.1.2.3	ENROLLMENT DATA MANAGER.....	63
A-3.1.2.4	NOTIFICATION SERVICES	63
A-3.2	CARD MANAGEMENT SYSTEM.....	64
A-3.3	DUPLICATE CHECKING USING BIOMETRICS	65
A-3.4	FEDERATED ID GATEWAY	65
A-3.5	CERTIFICATE AUTHORITY.....	66
A-3.6	HOTLIST MANAGER	66
A-3.7	CARD PRODUCTION FACILITY	66
A-3.8	ISSUANCE STATION.....	67
A-3.9	IDENTITY MANAGEMENT SECURITY MEASURES	68
A-3.10	CREDENTIALS	73
A-3.11	ACCESS CONTROL SYSTEM REQUIREMENTS.....	74
A-3.12	AIRPORT ACCESS CONTROL CREDENTIALS.....	75
A-3.12.1	STATIC PRINTED MEDIA	76
A-3.12.2	PERSONALIZED INFORMATION	77
A-3.13	SECURITY FEATURES.....	81
A-3.14	WRITEABLE AND RE-WRITEABLE UNPROTECTED MEDIA.....	81
A-3.14.1	MAGNETIC STRIPE.....	81
A-3.15	OPTICAL MEMORY	82
A-3.16	ELECTRICAL INTERFACE TECHNOLOGIES	83
A-3.16.1	CONTACT (ISO/IEC 7816)	83
A-3.16.2	CONTACTLESS	83
A-3.16.3	ID TOKEN CHIP TECHNOLOGIES	87
A-3.16.4	SMART CARDS.....	89
A-3.16.5	MULTIPLE TECHNOLOGY AND MULTIPLE INTERFACE CARDS.....	89
A-3.17	INTEROPERABLE CREDENTIALS	92
A-3.17.1	APPLICABILITY OF INTEROPERABLE CREDENTIALS TO AIRPORTS	93
4	PHYSICAL ACCESS CONTROL SYSTEMS, PACS.....	95
4.1	OVERVIEW	95
4.2	PACS MAIN COMPONENTS.....	97

4.2.1	CARDS.....	97
4.2.2	CARD READER	99
4.2.4	FIELD CONTROLLERS.....	103
4.2.5	PACS SERVER & APPLICATION SOFTWARE: MAIN FUNCTIONS OVERVIEW*.....	105
4.2.5.1	PACS SOFTWARE	106
4.2.5.2	PACS SERVER HARDWARE	108
4.2.5.3	PACS CLIENT WORKSTATIONS	109
4.3	REGISTERING PHYSICAL ACCESS PRIVILEGES - GENERAL PROCESS	109
4.4	INTEGRATION TOOL KIT - SOFTWARE DEVELOPMENT KIT	110
ANNEX 4 SECTION FOUR ANNEXES		111
A-4.1	BIOMETRICS IN PHYSICAL ACCESS CONTROL SYSTEMS	111
A-4.1.1	BIOMETRICS OVERVIEW	111
A-4.1.2	BIOMETRICS IN AIRPORTS – LEGAL, REGULATORY & POLICY BACKGROUND	112
A-4.1.2.1	GENERAL BIOMETRIC PROCESS.....	113
A-4.1.3	IMPLEMENTATION	115
A-4.1.3.1	BIOMETRIC ENROLLMENT AND TRAINING CONSIDERATIONS	115
A-4.1.3.2	INTERFACE BIOMETRICS TO EXISTING AND LEGACY ACCESS CONTROL SYSTEMS	116
A-4.1.3.3	BIOMETRIC READER PERFORMANCE CONSIDERATIONS.....	118
5	INTRUSION DETECTION SYSTEMS	121
5.1	INTRODUCTION	121
5.2	INTRUSION DETECTION AND TRACKING.....	121
5.2.1	INTRUDER CHARACTERISTICS.....	122
5.2.2	INTRUDER DETECTION	122
5.2.3	ALARM GENERATION.....	122
5.2.4	INTRUDER CLASSIFICATION	123
5.2.5	INTRUDER TRACKING.....	123
5.2.6	PERFORMANCE MEASURES	123
5.3	SECURITY FORCE TRACKING	124
5.4	INTRUSION ASSESSMENT AND SURVEILLANCE.....	124
5.4.1	CAMERA CHARACTERISTICS	124
5.4.2	CAMERA CONTROL	125
5.4.3	INTRUSION ASSESSMENT	125
5.4.4	PERFORMANCE MEASURES	125
5.5	LIGHTING REQUIREMENTS	125
5.6	INTRUSION DETECTION AND TRACKING TECHNOLOGIES.....	126
5.6.1	VIDEO MOTION DETECTION.....	127
5.6.2	VIDEO-BASED TRACKING	128
5.6.3	RADAR SYSTEMS.....	129
5.6.4	LADAR SYSTEMS	132
5.6.5	ACTIVE INFRARED (EXTERIOR).....	132
5.6.6	ACTIVE INFRARED (INTERIOR).....	133
5.6.7	PASSIVE INFRARED (INTERIOR).....	133
5.6.8	FENCE VIBRATION	133
5.6.9	FIBER-OPTIC CABLE.....	134
5.6.10	UNDERWATER FIBER-OPTIC NETTING	134
5.6.11	BURIED PRESSURE LINE SENSOR	134
5.6.12	PORTED COAX BURIED CABLE	135

5.6.13	TAUT WIRE.....	135
5.6.14	BI-STATIC MICROWAVE	135
5.6.15	OTHER TECHNOLOGIES	136
5.7	REFERENCE DOCUMENTS	136
6	VIDEO SURVEILLANCE.....	139
6.1	VIDEO SURVEILLANCE, MANAGEMENT, RECORDING AND ANALYTICS.....	139
6.2	VIDEO SURVEILLANCE PERFORMANCE.....	143
6.3	APPLICATIONS	146
6.3.1	OUTER PERIMETER.....	146
6.3.2	LANDSIDE TERMINAL ROADWAYS	146
6.3.3	VEHICLE ACCESS GATES	148
6.4	LIGHTING.....	150
6.5	VIDEO MANAGEMENT	153
6.5.1	EDGE ARCHITECTURE, TRANSMISSION BANDWIDTH, AND DIGITAL VIDEO STORAGE	153
6.5.2	VIDEO ANALYTICS	154
6.5.3	DIGITAL VIDEO RECORDING - RAID, NAS, AND SAN.....	157
6.5.4	VIDEO SERVERS	159
7	SECURITY OPERATIONS CENTER (SOC).....	161
7.1	INTRODUCTION	161
7.2	FACILITIES: STANDARD SECURITY OPERATIONS CENTER.....	162
7.2.1	FACILITIES: STANDARD SOC DESIGN / BUILD / OPERATION CONSIDERATIONS	163
7.2.2	FACILITIES: SOC SUPPORTING PACS COMMUNICATIONS INFRASTRUCTURE	163
7.3	FUNCTION: SECURITY OPERATIONS CENTER (SOC) REQUIREMENTS.....	163
7.4	PHILOSOPHY: SOC AND SITUATIONAL AWARENESS	164
7.4.1	PHILOSOPHY: CONTINUING DOMAIN AWARENESS IN THE SOC	164
8	COMMUNICATIONS INFRASTRUCTURE	167
8.1	ESTABLISHING A COMMUNICATIONS INFRASTRUCTURE	167
8.2	COMMUNICATION INFRASTRUCTURE RELATIONSHIPS	168
8.2.1	COMMUNICATIONS INFRASTRUCTURE FUNCTIONALITY	169
8.3	COMMUNICATIONS CHARACTERISTICS	171
8.4	NETWORK DESIGN.....	172
8.4.1	DESIGN OBJECTIVES	172
8.4.2	LAN PROTOCOLS	173
8.4.3	OSI MODEL	174
8.4.4	TOPOLOGIES	175
8.4.5	VLANs.....	176
8.4.6	BANDWIDTH MANAGEMENT.....	177
8.4.7	QUALITY OF SERVICE (QOS) ISSUES.....	178
8.4.8	IP VOICE.....	178
8.4.9	MULTICASTING	179
8.4.10	VPN.....	179
8.4.11	WIRELESS COMMUNICATIONS	180
8.4.12	NETWORK SECURITY	184
8.5	PHYSICAL CABLE PLANT	186
8.5.1	CABLE PLANT MIGRATION STRATEGY	187
8.5.2	WIRE AND CABLE INSTALLATION	188

8.6	PHYSICAL PROTECTION OF NETWORK ASSETS	189
9	GENERAL ACQUISITION RELATED CONSIDERATIONS	191
9.1	INTRODUCTION	191
9.2	REGULATORY REQUIREMENTS	191
9.2.1	FEDERAL, STATE, AND LOCAL REGULATORY REQUIREMENTS	191
9.3	SYSTEM ACQUISITION PHASE.....	193
9.3.1	SYSTEM DESIGN	193
9.3.2	SYSTEM DESIGN OBJECTIVES	193
9.3.3	LEGACY SYSTEM INTEGRATION.....	195
9.3.4	SYSTEM SPECIFICATION AND SELECTION	195
9.4	SYSTEM INSTALLATION PHASE	196
9.5	IMPLEMENTATION PHASING CONSIDERATIONS.....	197
9.6	SYSTEM DOCUMENTATION	197
9.6.1	AS-BUILT DRAWINGS AND BILL OF MATERIALS	197
9.6.2	OPERATIONAL PROCEDURES FORMAT AND CONTENT.....	197
9.7	TRAINING MANUALS AND COURSES.....	198
9.7.1	ISSA OPERATOR TRAINING	198
9.7.2	SYSTEMS ADMINISTRATOR TRAINING	198
9.7.3	MAINTENANCE TRAINING.....	199
9.7.4	BIOMETRICS – SPECIAL USER TRAINING CONSIDERATIONS.....	199
9.8	SYSTEM TEST, VERIFICATION AND VALIDATION.....	199
9.8.1	SYSTEM TEST	200
9.8.2	SPECIAL BIOMETRIC SUBSYSTEM TESTING AND CERTIFICATION.....	203
9.9	WARRANTY REQUIREMENTS.....	204
9.10	SYSTEM LOGISTICS SUPPORT	204
9.10.1	MAINTENANCE CONSIDERATIONS	204
ANNEX 9	SECTION NINE ANNEXES	209
A-9.1	REGULATIONS, CODES, STANDARDS AND GUIDELINES	209
A-9.1.1	FEDERAL, STATE, AND LOCAL	209
A-9.1.1.1	CODE OF FEDERAL REGULATIONS (CFR)	209
A-9.1.1.2	TRANSPORTATION SECURITY ADMINISTRATION (TSA)	209
A-9.1.1.3	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST).....	209
A-9.1.1.4	DEPARTMENT OF DEFENSE (DoD).....	209
A-9.1.1.5	OTHER AGENCIES.....	210
A-9.1.2	INDUSTRY AND INTERNATIONAL STANDARDS.....	210
A-9.1.2.1	CONSTRUCTION SPECIFICATIONS INSTITUTE (CSI), MASTERSPEC (2004).....	210
A-9.1.2.2	ELECTRONIC INDUSTRIES ALLIANCE (EIA)	210
A-9.1.2.3	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE).....	210
A-9.1.2.4	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)	211
A-9.1.2.5	NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA)	211
A-9.1.2.6	NATIONAL FIRE PROTECTION ASSOCIATION (NFPA).....	211
A-9.1.2.7	UNDERWRITERS' LABORATORIES (UL)	211
A-9.1.3	OTHER REFERENCES	211
A-9.2	OPERATIONAL AVAILABILITY, RELIABILITY, AND MAINTAINABILITY	212
A-9.2.1	OPERATIONAL AVAILABILITY.....	212
A-9.2.2	OPERATIONAL RELIABILITY.....	214
A-9.2.3	OPERATIONAL MAINTAINABILITY	215

A-9.2.4	GUIDANCE FOR BIOMETRIC DEVICE OPERATIONAL AVAILABILITY.....	215
A-9.3	FINAL AS-BUILT DRAWINGS AND LIST OF MATERIALS (LOM).....	216
A-9.3.1	DOOR TEST SCHEDULE	219
A-9.3.1.1	NORMAL ACCESS	219
A-9.3.1.2	LOCAL GRANT.....	219
A-9.3.1.3	REJECTED ACCESS	219
A-9.3.2	DOOR CONTACT	219
A-9.3.2.1	“CARD READER” DOOR	219
A-9.3.2.2	“CONTACT ONLY” DOOR.....	219
A-9.3.2.3	TAMPER SWITCH.....	219
A-9.3.2.4	SUPERVISED INPUTS.....	220
A-9.3.2.5	COMMUNICATION SUPERVISION	220
A-9.3.2.6	REMOTE LOCKING AND UNLOCKING OF DOORS.....	220
A-9.3.2.7	FIRE ALARM OVERRIDE (MAGNETIC LOCK DOORS ONLY).....	220
A-9.3.2.8	BATTERY BACKUP	220
A-9.3.2.9	GRAPHIC MAP DISPLAY OF ALARMS	220
A-9.3.2.10	PHYSICAL INSPECTION OF DOOR HARDWARE	220
A-9.3.3	PHYSICAL INSPECTION OF PACS PANEL AND POWER SUPPLIES	221
MEMBERSHIP		223
APPENDIX I STANDARDS		I-1
I.1 IDENTIFICATION CARD TECHNOLOGY STANDARDS (MAGNETIC STRIPE AND SMART CARD)...		I-2
I.1.2	PHOTOS	I-3
I.1.3	BARCODES	I-3
I.1.4	OPTICAL MEMORY	I-3
I.2 CONTACT INTERFACES		I-4
I.3 CONTACTLESS INTERFACES		I-6
I.3.1	COUNTRY-SPECIFIC ISSUES FOR CONTACTLESS.....	I-7
I.4 SECURITY AND ASSURANCE STANDARDS		I-7
I.5 IDENTITY DOCUMENT STANDARDS		I-8
I.6 BIOMETRIC STANDARDS		I-8
I.6.1	BIOMETRIC APPLICATION INTERFACE STANDARDS	I-8
I.6.2	BIOMETRIC APPLICATION PROFILE STANDARDS.....	I-10
APPENDIX II MAGNETIC STRIPE TRACK USE		II-1
II.1 FINANCIAL CARDS		II-1
II.2 DRIVER'S LICENSES (USA)		II-2
II.3 SEIWG-012 PHYSICAL ACCESS CONTROL (DoD)		II-3
II.4 FEDERAL AGENCY SMART CREDENTIAL NUMBER (GSC-IAB)		II-4
APPENDIX III SECURITY DEVICE ATTACHMENT		III-1
III.1 INTRODUCTION		III-1
III.2 THREAT LEVELS		III-1
III.3 THREAT TYPES		III-1
III.4 PRINTING		III-1
III.5 INKS		III-3
III.6 SUBSTRATE INCLUSION		III-4
III.7 OPTICALLY VARIABLE DEVICES (OVD)		III-4

III.8	ADDITIONAL FEATURES	III-6
APPENDIX IV PACS INTEGRATION TO PHYSICAL IDS		
IV.1	PACS INTEGRATION TO PHYSICAL INTRUSION DETECTION SYSTEM	IV-1
IV.2	DATABASE DESIGN CONSIDERATIONS.....	IV-2
IV.3	EXTERNAL IT INTERFACES	IV-5
IV.4	PACS FIPS 201 MIGRATION.....	IV-5
IV.5	CENTRALIZED PACS DATABASE	IV-6
IV.6	DISTRIBUTED PACS DATABASE.....	IV-6
IV.7	HOST SELECTION, CONFIGURATION AND SIZING.....	IV-7
IV.8	HOST AVAILABILITY, REDUNDANCY AND RAID	IV-8
IV.9	CLOUD COMPUTING	IV-8
IV.10	CHANGE MANAGEMENT: DOCUMENTATION AND TRAINING	IV-9
IV.11	PACS APPLICATIONS	IV-9
IV.12	SECURITY CERTIFICATION AND ACCREDITATION	IV-10
APPENDIX V GLOSSARY		
		V-1
APPENDIX VI APPENDIX REFERENCES		
		VI-1
APPENDIX VII VISUAL SECURITY FOR GOVERNMENT CREDENTIALING		
		VII-1

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.