

RTCA, Inc.
1150 18th Street NW, Suite 910
Washington, DC 20036
USA

Standards for Airport Security Access Control Systems

The RTCA SC-224 Release of DO-230K is dedicated to the memory of J. Leonard Wood, LTC (USA-Ret). Upon his retirement from the military (recognized as a Viet Nam hero), he began a civil airport career with the Maryland Aviation Administration, advancing to Associate Administrator – Operations. As a long-time aviation consultant, he designed airport security systems for 34 airports and 3 air carriers. He was one of the early participants in the development of DO-230 and was active in later version until recent years. Mr. Wood passed January 1, 2020.

DO-230K: Airport Security Access Control Systems – Dedicated to J. Leonard Wood, LTC (USA-Ret)

RTCA DO-230K
June 17, 2021

Prepared by: SC-224
© 2021 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 Special Committee 224 (SC-224) and approved by the RTCA Program Management Committee (PMC) on June 17, 2021.

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 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.
- 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.

DISCLAIMER

This publication is based on material submitted by various participants during the SC approval process. Neither the SC nor RTCA has made any determination whether these materials could be subject to valid claims of patent, copyright, or other proprietary rights by third parties, and no representation or warranty, expressed or implied is made in this regard. Any use of or reliance on this document shall constitute an acceptance thereof "as is" and be subject to this disclaimer.

This Page Intentionally Left Blank

EXECUTIVE SUMMARY

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 with substantive changes in the biometrics, credentialing, integration, procurement, and video surveillance sections and minor changes throughout other sections of the document. In addition, two new sections were added to the document covering facilitation and cybersecurity. Advances in Biometrics technology, Artificial Intelligence (AI), neural networks, and facial recognition have been included in the biometrics section including international plans and references.

The credentialing section was updated to include more streamlined processes that have been enacted by airport operators including enhancements to the criminal history records check, the credential revocation process, and guidance on privacy protection based on the increased amount of personal identifiable information that is collected for the issuance of credentials. The integration section was reorganized to focus on airport needs, integration strategies, prioritization of activities, and considerations for some of the current trends that affect airport operators' decisions when selecting their access control systems. A notional checklist is provided as guidance in this section. The procurement section was revamped to address more generic process with the focus on project deliverables and timelines. Procurement strategies and consideration guidance, regulatory considerations, contract negotiations, acquisition strategies, installation and implementation, testing, training, maintenance, and operational considerations guidance have been included in this section. The video surveillance section has been updated and revamped with the focus on the architecture of video surveillance in support of airport operations. Video surveillance architectural guidance in support of physical access control systems, perimeter intrusion detection systems and its integration into the security operations center have been included along with emerging technological considerations such as cloud storage.

One of the new additions to DO-230 is the facilitation sections that provides guidance for border control processes to expedite movement of passengers, crew personnel, baggage and cargo, and other services by airport operators thru their facility. This section introduces facility security design considerations, the establishment of security corridors, documentation and credentialing procedures, recommended facilitation best practices. The area of cybersecurity continues to evolve at a rapid pace and the new cybersecurity section provides insight into some of the threat types that could be by airport operators. The cybersecurity section references emerging trends in layered defense of airport security assets and provides guidance on detection and mitigation steps, cybersecurity risk management, trust frameworks and the concepts of zero trust, best practices for airport organizations. The cybersecurity section will continue to evolve with future releases of DO-230 as the threat landscape continues to change.

For readers of the credentialing section, the National Institute of Standards and Technology (NIST) continues to provide guidance on identity verification. The guidance pertains to Federal Government users and while not applicable to airport operators, RTCA SC-224 recommends readers familiarize themselves on possible impacts to their credentialing and airport access policies.

The nature of video surveillance equipment changes due to technological enhancements/obsolesce and standards drove the video surveillance section updates. Within other previously updated sections, privacy concerns continued to be raised as they relate to video surveillance using closed circuit television (CCTV) systems, 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.

In general, privacy concerns have been raised in other sections including credentialing, cybersecurity, and facilitation sections.

As in previous releases of DO-230, RTCA SC-224 received input from the TSA, airports, and industry representatives for inclusion in the revised credentialing section.

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. RTCA SC-224 has deemed this topic area to be outside the scope of this document but may warrant further investigation in a future release.

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) Privacy Office continues to provide publications on topics such as border security, cybersecurity, transportation security on their website.

This RTCA DO-230K document contains forward-thinking references to technology, processes and guidance which 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.

Finally, the document provides information on technology trends in PACS, access card technology, video surveillance, wireless and physical security information management (PSIM) systems 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 facilities.

Further, the information contained herein represents the experience of airport operators and their professional organizations (Airport Consultants Council (ACC)) and industry associations (Airports Council International-North America (ACI-NA)), as well as security technology industry representatives (i.e., standards organizations, industry organizations, vendors, integrators); airline industry bodies (International Air Transport Association (IATA) and Airlines for America (A4A)); and aviation/airport regulatory bodies such as the FAA and TSA.

This document was prepared by RTCA SC-224, which included in its membership representatives from all 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
1.1	Purpose.....	1
1.2	History	1
1.3	Scope.....	2
1.4	Methodology.....	2
1.5	High-Level Concept of Operations (ConOps).....	3
1.5.1	Communications ConOps	4
1.5.2	Credentialing ConOps.....	4
1.5.3	Biometric ConOps	4
1.5.4	PACS ConOps	5
1.5.5	Perimeter Intrusion Detection ConOps.....	5
1.5.6	Video ConOps.....	6
1.5.7	SOC ConOps.....	7
1.5.8	Integration ConOps.....	8
1.6	System Overview	8
1.6.1	Communications	9
1.6.2	Credentialing.....	9
1.6.3	Biometrics	10
1.6.4	PACS.	10
1.6.5	Perimeter Intrusion Detection.....	10
1.6.6	Video.....	12
1.6.7	SOC.....	12
1.6.8	Integration.....	13
1.7	Standards, Regulatory Requirements and Recommended Practices.....	14
1.8	Cybersecurity	15
1.8.1	National Security Initiatives	15
1.8.2	FICAM Cyber Security Programs	15
1.8.3	EOP-OMB Cloud Computing Initiative	15
1.8.4	SOC Participants.....	16
1.8.5	Aircraft Operators	17
1.8.6	Federal Agencies.....	17
1.8.7	LEOs.....	17
1.8.8	Incident Response Posts.....	18
1.9	Integration.....	18
1.9.1	Trade Studies / Design Trade Offs.....	18
1.9.2	Configuration Management / Interfacing / Integration / Migration Issues	18
1.10	Facilitation	19
2	CREDENTIALING	21
2.1	Introduction and Purpose	21
2.2	Federally Regulated Credentialing Process	23
2.2.1	Application Process	24
2.2.2	Identify Verification Process	24
2.2.3	Background and Security Check Process.....	25
2.2.4	Adjudication Management Process.....	26

2.2.5	Training Function	28
2.2.6	Credential Issuance Process.....	28
2.2.7	Lifecycle Credential Management.....	28
2.2.8	Credential Regulatory / Compliance Requirements.....	30
2.2.9	Other Function	30
2.2.10	Typical Credentialing System Interfaces	30
2.3	Credentialing Implementation Systems	32
2.3.1	Manually Managed Credentialing System.....	32
2.3.2	Partially Integrated Based on Existing Computer PACS.....	33
2.3.3	Fully Automated Management Systems (IDMS).....	33
2.4	Contrasting Automation Approaches.....	34
2.5	Cybersecurity in Credentialing	35
2.6	Credentialing Trends.....	36
2.6.1	Next Generation Identification (NGI).....	36
2.6.2	Enhanced Criminal History Checks.....	36
2.6.3	FIPS 201	36
2.6.4	REAL ID.....	37
2.6.5	Inspection of Credential Holders	37
2.6.6	Privacy Protection	37
2.7	Credentialing Implementation Checklist	38
2.8	Credentialing Operational Checklist.....	38
3	BIOMETRICS.....	41
3.1	Introduction and Background	41
3.1.1	Introduction.....	41
3.1.2	Reasons to Use Biometrics	41
3.1.3	Basic Functions.....	42
3.1.4	Biometric Modalities	42
3.1.5	Legislative and Regulatory Requirements	44
3.1.6	Recent Technology Advances.....	45
3.2	Biometric Applications	46
3.2.1	Criminal History Records Check (CHRC).....	46
3.2.2	De-duplication at Enrollment.....	47
3.2.3	Physical Access Control	47
3.2.4	Logical Access to Security Systems	50
3.2.5	ID Verification.....	50
3.3	Biometric Considerations.....	51
3.3.1	False Rejection Rate (FRR)	52
3.3.2	False Acceptance Rate (FAR).....	52
3.3.3	Equal Error Rate (EER)	52
3.3.4	Failure to Enroll (FTE)	52
3.3.5	Failure to Acquire (FTA).....	53
3.3.6	Throughput Rate	53
3.3.7	Environmental Conditions	54
3.3.8	Usability.....	54
3.3.9	Anti-spoofing and Liveness Detection.....	55
3.4	Enrollment Considerations.....	55
3.4.1	Quality	55
3.4.2	Test Verification	56

3.4.3	Training (Enrollees and Operators)	56
3.4.4	Retention of Original Biometric Identifiers	56
3.5	Managing Exceptions.....	57
3.6	Privacy and Data Security Considerations.....	57
3.6.1	Encrypted in Transit and at Rest.....	59
3.6.2	Digital Signatures or other Data Protection mechanisms	59
3.7	Threat Vectors and Mitigation Options	59
3.7.1	Sensor Spoofing.....	59
3.7.2	Data Manipulation or Replacement	60
3.7.3	False Identity Claim at Enrollment.....	60
3.7.4	Imposter Attempts.....	60
3.8	Biometric Standards.....	61
3.8.1	Technical Interfaces.....	62
3.8.2	Data Formats.....	63
3.8.3	Implementations.....	64
3.8.4	Testing and Reporting.....	65
3.9	Future Biometric trends	66
3.10	Biometrics Checklist.....	68
4	PHYSICAL ACCESS CONTROL SYSTEM (PACS).....	69
4.1	Overview.....	69
4.2	PACS Main Components	69
4.2.1	Emerging PACS Technologies – Cards and Readers	71
4.2.2	Near Field Communication (NFC)	71
4.2.3	Cloud Computing in Physical Security.....	71
4.2.4	Card Types.....	72
4.2.5	Personal Identification Number (PIN) Utilization	74
4.2.6	Card Technologies	75
4.2.7	Card/Credential Reader Considerations.....	76
4.2.8	Portal Door Hardware	79
4.2.9	Field Controllers	79
4.2.10	PACS Server & Application Software: main Functions Overview	82
4.2.11	Special PACS Use Cases	85
4.3	Regulatory Requirements and Industry Standards.....	87
4.3.1	Standards, Regulations and Guidelines Applicable to Airport Access Control Systems.....	87
4.3.2	Environmental Impact to Airport PACS.....	90
4.4	System Design Issues Overview (Reference ConOps).....	90
4.4.1	Throughput at Different Boundary Areas Entry and Exit.....	90
4.4.2	System Design Considerations – Threats.....	90
4.4.3	Hardware.....	91
4.4.4	Software	91
4.4.5	Electrical	91
4.4.6	Environmental.....	91
4.4.7	Maintenance.....	91
4.5	Portal Operation.....	92
4.5.1	Portal Position Switch.....	92
4.5.2	Interior Doors.....	93
4.5.3	Exterior Doors.....	93
4.5.4	Fire Rated Doors	93

4.5.5	Automated Exit Lane Breach Control.....	94
4.5.6	Rotating Portals.....	98
4.5.7	Mantraps	98
4.5.8	Rollup Doors.....	98
4.5.9	Vehicle Barriers	98
4.5.10	Key and Lock Technologies	99
4.5.11	Other.....	100
4.5.12	Auditing and Reporting.....	100
4.5.13	Server Configuration.....	100
4.5.14	Power Considerations	101
4.6	Authentication Mechanisms; Multiple Authentication and Security Factors	102
4.6.1	PIN-to-PACS as Single Factor Knowledge	104
4.6.2	PIN-to-Card Operation.....	105
4.6.3	Card with PIN-to-PACS Operation	105
4.6.4	Authentication IT Infrastructure with PKI.....	106
4.6.5	PACS System Operator Authentication.....	107
4.6.6	Data Protection: Data in Transit	108
4.7	PACS Technology Trends	108
4.7.1	Multifactor Authentication, Stand Alone, Self-Contained Reader	108
4.7.2	Card-Reader Mutual Authentication.....	110
4.7.3	Virtualization	110
4.8	Interfaces with Other Systems	114
4.8.1	Access Alarms	115
4.8.2	Intrusion Alarms	115
4.8.3	Portal Operations	115
4.9	Pilot Access.....	119
4.10	Physical Access Control System (PACS) Checklist.....	120
5	PERIMETER INTRUSION DETECTION.....	125
5.1	Perimeter Intrusion Detection System Overview.....	125
5.1.1	Mission.....	125
5.1.2	Risk and Needs Assessment.....	126
5.2	Regulatory Requirements.....	127
5.3	Threats/Vulnerabilities.....	127
5.4	Current Practices.....	128
5.4.1	Fencing.....	128
5.4.2	Sensing Technology.....	128
5.4.3	Patrol.....	129
5.4.4	Perimeter Maintenance	129
5.4.5	Best Practices.....	130
5.4.6	Perimeter Systems Product Testing	130
5.5	Requirements	130
5.5.1	Requirements Overview.....	130
5.5.2	Requirements Traceability	130
5.5.3	Typical PIDS Requirements	131
5.6	System Design Considerations	133
5.6.1	Design Process.....	133
5.6.2	System Performance	133
5.6.3	Design Factors and Constraints	136

5.6.4	Tolerance for Change.....	137
5.7	Industry Standards	138
5.8	Current Technology	144
5.8.1	Introduction.....	144
5.8.2	Assess / Identify / Classify.....	157
5.8.3	Track / Locate	157
5.8.4	Other Technologies.....	160
5.9	Technology Trends	160
5.9.1	Wireless Technologies.....	161
5.9.2	Physical Security Information Management (PSIM) Systems.....	161
5.10	PIDS Integration	161
5.11	Staffing, Training and Sustainment (Maintenance)	162
5.11.1	Staffing Considerations.....	162
5.11.2	Perimeter Security Training Considerations.....	163
5.11.3	Sustainment Considerations.....	163
5.12	References to Previous PIDs Sections	163
5.13	Perimeter Intrusion Detection Checklist.....	163
6	VIDEO SURVEILLANCE SYSTEMS	165
6.1	System Overview	165
6.2	Application of Video Surveillance Systems	166
6.2.1	Alarm Monitoring and Assessment	166
6.2.2	Perimeter and Surveillance	168
6.2.3	Forensic Review	169
6.2.4	Integration with Other Systems	170
6.3	Design Considerations	171
6.3.1	System Design	171
6.3.2	Imager Operational Performance.....	172
6.3.3	Imaging Sensor Type.....	173
6.4	Video Surveillance System Architecture.....	173
6.4.1	Video Management Systems (VMS).....	175
6.4.2	Recorders	176
6.4.3	Clients	179
6.4.4	Storage	179
6.4.5	Cameras	182
6.4.6	Microphones	191
6.5	Video Analytics	191
6.5.1	Applications.....	192
6.5.2	Edge-based Analytics.....	194
6.5.3	Server-based Analytics	194
6.5.4	Cloud-based Analytics.....	195
6.5.5	Artificial intelligence	195
6.6	Lighting.....	195
6.7	Information Technology (IT) and Network Considerations	198
6.7.1	Bandwidth Utilization.....	198
6.7.2	VLANs and Firewalls	199
6.7.3	Cybersecurity considerations	200
6.7.4	Virtualization	200
6.8	Standards.....	201

6.8.1	Open Standards	201
6.8.2	Standards Groups	201
6.8.3	Networking Standards.....	202
6.8.4	US and International Video Standards.....	202
6.8.5	Encoding	203
6.9	Regulations	204
6.10	System Testing.....	204
6.10.1	Performance Metrics.....	205
6.10.2	Analytics Testing	206
6.11	Technology Trends	206
6.12	Video Surveillance Checklist.....	207
7	SECURITY OPERATIONS CENTER (SOC)	209
7.1	Typical Security Operations Center.....	212
7.1.1	Facilities: Standard SOC Design / Build / Operation Considerations.....	212
7.1.2	Facilities: SOC Supporting PACS Communications Infrastructure	213
7.2	Security Operations Center (SOC) Requirements	213
7.2.1	Displaying Information in the SOC	213
7.3	SOC and Situational Awareness	214
7.3.1	Continuing Domain Awareness in the SOC	215
7.4	SOC Checklist.....	215
8	INTEGRATION.....	217
8.1	Overview.....	217
8.2	Analysis of the Airport's Needs	217
8.2.1	Current Requirements	217
8.2.2	Future Requirements.....	218
8.2.3	Gap Analysis.....	218
8.3	Integration Strategy.....	219
8.3.1	Overview.....	219
8.3.2	Designing the Target Architecture.....	219
8.3.3	Priority Setting & Delivery Sequencing	223
8.4	Integration Trends.....	225
8.5	Planning Tips	225
8.6	Integration Checklist.....	226
9	COMMUNICATIONS INFRASTRUCTURE	227
9.1	Introduction – Overview	227
9.2	System Requirements Summary	228
9.2.1	Wired Communication Systems	228
9.2.2	Wireless Communications Systems.....	229
9.2.3	Commercial Services	233
9.2.4	Wireless IT Networks, also known as Wireless LANs (WLANs).....	233
9.3	Regulatory Requirements and Standards	234
9.3.1	FCC Role	235
9.3.2	Spectrum Considerations	235
9.4	Threats	236

9.4.1	Public Key Infrastructures (PKIs).....	238
9.5	Current Practices.....	238
9.6	Design Objectives.....	239
9.6.1	Communications Infrastructure.....	239
9.6.2	Network Standards.....	240
9.6.3	Network Infrastructure Relationships.....	241
9.6.4	Communications Functionality.....	242
9.7	System Design Considerations.....	243
9.7.1	Performance.....	244
9.7.2	LAN Protocols.....	245
9.7.3	OSI Model.....	245
9.7.4	Topologies.....	246
9.7.5	VLANs.....	248
9.7.6	Bandwidth Management.....	248
9.7.7	Quality of Service (QoS) Issues.....	249
9.7.8	IP Voice.....	249
9.7.9	Multicasting.....	250
9.7.10	Virtual Private Network (VPN).....	251
9.8	Network Backbone and Infrastructure.....	251
9.9	Device Wiring.....	252
9.9.1	Cabling Management.....	252
9.9.2	Cable Plant Migration Strategy.....	253
9.9.3	Wire and Cable Installation.....	253
9.9.4	Fiber Optic Backbone Cabling.....	254
9.9.5	Structured Cabling.....	255
9.9.6	End Point Connections.....	260
9.9.7	Complying with Standards.....	261
9.9.8	Labeling.....	261
9.9.9	Telecommunication Rooms (TRs).....	262
9.10	Wireless Networks and Devices.....	263
9.10.1	Wireless Communications.....	263
9.10.2	Wireless LANs (WLAN).....	264
9.10.3	WiFi Wireless LANs.....	266
9.10.4	WiMAX.....	267
9.10.5	Long Range WiFi Communications.....	268
9.10.6	Radio Frequency Identification (RFID).....	268
9.10.7	Near-Field Communications (NFC).....	269
9.10.8	Radio over IP (RoIP).....	270
9.11	Privacy and Data Security Considerations.....	271
9.11.1	Network Security Standards and Guidelines.....	271
9.11.2	Transmission and Data Security.....	271
9.11.3	Network Security.....	272
9.11.4	Cybersecurity.....	272
9.12	Trends.....	276
10	GENERAL ACQUISITION-RELATED CONSIDERATIONS.....	277
10.1	Introduction.....	277
10.2	Airport Needs Assessment.....	277
10.2.1	Assess Current Capabilities and Systems.....	277

10.2.2	Gap Analysis.....	277
10.2.3	Identify Target Outcomes	278
10.3	Procurement Strategy.....	278
10.3.1	Considerations	278
10.3.2	Options.....	279
10.3.3	Best Practices.....	280
10.4	Funding Acquisition.....	282
10.4.1	Assessment.....	282
10.4.2	Source (Local, State & Federal).....	282
10.4.3	Business Case	282
10.5	Procurements Execution	283
10.5.1	Scope Preparation	283
10.5.2	Disclosure of Sensitive Security Information (SSI).....	284
10.5.3	Proposal Assessment.....	285
10.5.4	Provider Selection.....	285
10.5.5	Contract Negotiations	285
10.6	System Design	285
10.6.1	Guiding Principals	286
10.7	System Installation.....	288
10.7.1	Implementation Phasing Considerations.....	288
10.7.2	Preparation and Installation	289
10.7.3	Migration and Cutover.....	290
10.8	Testing and Acceptance Considerations	290
10.8.1	Test Strategy	290
10.8.2	System Test Development	291
10.8.3	System Test Procedure Development (STProc).....	291
10.8.4	Test Execution	292
10.9	Training Courses.....	294
10.9.1	ISSA Operator Training.....	294
10.9.2	Systems Administrator Training.....	295
10.9.3	Maintenance Training.....	295
10.10	System Documentation	295
10.10.1	As-Built Drawings & Bill of Materials.....	295
10.10.2	Operational Procedures Format and Content.....	296
10.10.3	Training Manuals.....	296
10.11	Warranty & Maintenance.....	296
10.11.1	Warranty Requirements	296
10.11.2	System Logistics	296
10.11.3	Maintenance Considerations	296
10.12	Procurement Checklist.....	297
11	FACILITATION.....	301
11.1	Preface	301
11.2	Introduction.....	301
11.3	Purpose.....	302
11.4	History / Background.....	303
11.5	System Overview (FAL).....	304
11.6	Major Elements.....	304
11.6.1	International Arrivals Facilities—Federal Inspection Services	304

11.6.2	Sterile Corridor System.....	305
11.6.3	CBP Primary Inspection	305
11.6.4	Baggage Claim.....	306
11.6.5	CBP Secondary Inspection and Processing	306
11.6.6	Transfer Passenger Re-check.....	306
11.6.7	Meeter/Greeter Lobby.....	306
11.6.8	CBP Administrative and Support Areas	306
11.7	Document Authentication Process	307
11.7.1	Document Reader Requirements:	307
11.7.2	Technical Requirements.....	307
11.8	ID Verification.....	308
11.8.1	ICAO TRIP	308
11.9	Biometric Verification Process	309
11.9.1	Technical Standards Regarding Certain Elements Include.....	309
11.10	Quality Control/Quality Assurance.....	310
11.10.1	General recommendations	310
11.11	Federal & International Requirements.....	311
11.12	Methodology.....	312
11.13	Essential Elements	312
11.14	Passenger Assessments Background.....	313
11.15	Technical Advances	314
11.16	Best Practices.....	315
11.17	Implementation List.....	316
11.18	Standards, Regulatory Requirement & Recommended Practices	316
12	CYBERSECURITY	317
12.1	Introduction.....	317
12.2	Types of Threats	317
12.3	Layered Approach to Cybersecurity	318
12.4	NIST Cybersecurity Framework.....	321
12.5	ICAO Aviation Cybersecurity	321
12.6	CANSO Cybersecurity.....	322
12.7	Zero Trust Architecture.....	323
12.8	Conclusion	324
13	MEMBERSHIP	327
	APPENDIX A - STANDARDS	A-1
A.1	Federal State and Local Standards	A-2
A.1.1	Code of Federal Regulations (CFR)	A-2
A.1.2	Transportation Security Administration (TSA)	A-2
A.1.3	National Institute of Standards and Technology (NIST)	A-2
A.1.4	Department of Defense (DoD).....	A-2
A.1.5	Other Federal Agencies.....	A-2
A.2	Industry and International Standards	A-3
A.2.1	Airports Council International (ACI)/International Air Transportation Association (IATA)	A-3
A.2.2	American National Standards Institute (ANSI) / Electronic Industries Alliance (EIA).....	A-3

A.2.3	Construction Specifications Institute (CSI), MasterSpec (2004)	A-3
A.2.4	Institute of Electrical and Electronics Engineers (IEEE)	A-3
A.2.5	International Civil Aviation Organization (ICAO)	A-3
A.2.6	International Organization for Standardization (ISO).....	A-4
A.2.7	National Electrical Manufacturers Association (NEMA)	A-4
A.2.8	National Fire Protection Association (NFPA)	A-4
A.2.9	Underwriters' laboratories (UL)	A-4
APPENDIX B - GLOSSARY		B-1
APPENDIX C – OTHER REFERENCES.....		C-1
APPENDIX D – INDENTITY MANAGEMENT SYSTEMS (IDMS).....		D-1
D.1	Overview.....	D-1
D.2	Components and functions.....	D-1
D.2.1	Authorized Signatory Functions	D-2
D.2.2	Trusted Agent Functions.....	D-2
D.2.3	Credential Issuing Functions.....	D-2
D.3	Optional Credentialing Capabilities.....	D-3
D.3.1	Asset/Vehicle Management	D-3
D.3.2	Infractions Management	D-3
D.3.3	Finance Management	D-3
D.3.4	Audit Management.....	D-3
D.3.5	Configurable Report Generation.....	D-3
D.3.6	Scheduling Management.....	D-4
D.3.7	Data Management/Record Keeping.....	D-4

TABLE OF TABLES

Table 1-1: Airport Security Areas of Concern, Threats and Countermeasures	11
Table 4-1: PACS Standard Components.....	70
Table 4-2: Contactless Smart Card vs. Proximity Card Technologies.....	73
Table 4-3: PACS & Level of Assurance.....	74
Table 5-1: Example of Key Performance Parameters.....	133
Table 5-2: System Type – Sensor Technology Pd Comparison	135
Table 5-3: Typical PIDS-related Standards	139
Table 5-4: Perimeter Sensors	145
Table 6-1: Redundant Array of Independent Disks (RAID) Levels	181
Table 6-2: Common Camera Types and Their Pixel Counts.....	183
Table 6-3: Angular and Linear Field Coverage for Camera-Lens Combinations.....	189
Table 6-4: Typical Illumination Standards	197
Table 9-1: Fiber Type vs. Speed and Distances.....	255
Table 9-2: TIA Cable Classifications and Standards	257
Table 9-3: ISO Cable Classifications and Standards	257
Table 9-4: IEEE WLAN Standards.....	264
Table 9-5: Characteristics of IEEE WLAN Standards.....	266
Table 9-6: Evolution of the 802.11 Standards	267

TABLE OF FIGURES

Figure 1-1: Notional Airport Layout (separated Domestic and International Areas)	3
Figure 1-2: Notional Perimeter Security and Zones	6
Figure 1-3: Notional Security Operations Center (SOC).....	7
Figure 2-1: Overview of Federal Credentialing Process for Airports.....	23
Figure 3-1: Generic Biometric Processes.....	48
Figure 4-1: Sample PACS Configuration	70
Figure 4-2: Sample PACS and IDMS Components.....	71
Figure 4-3: Cards and Card Data – Current Industry Trends.....	75
Figure 4-4: Physical Access Control Form Factors	76
Figure 4-5: Typical Master Key Schema	99
Figure 4-6: Reader to Controller Data Flow	104
Figure 4-7: Generic PKI-enabled PACS Configuration.....	107
Figure 4-8: Narrow Mullion Style Self-Contained Unit (left), Self-Contained Unit with Mortise Lock (center), Self-Contained Unit with Mortise Lock and Key Override (right)	109
Figure 5-1: Typical PIDS Progression	126
Figure 6-1: Components and Generic Architecture of a VSS.....	166
Figure 6-2: Spectral Regions Used by Visible and Infrared Imaging Sensors.....	183
Figure 6-3: Determining Pixel per Foot (PPF) Values.....	188
Figure 6-4: Camera Angular Coverage and Typical Performance Values.....	190
Figure 7-1: Typical SOC Information Flow Diagram.....	211
Figure 7-2: Examples of SOC Configurations – Small / Medium / Large.....	214
Figure 9-1: Airport Communications Diagram.....	227
Figure 9-2: Frequency Band Allocations	232
Figure 9-3: Spectrum Band and Frequency Assignment	236
Figure 9-4: Communication Relationship.....	242
Figure 9-5: Communication Services	242
Figure 9-6: OSI Stack	246
Figure 9-7: Network Topologies.....	246
Figure 9-8: Network Elements Configured for Redundancy	247
Figure 9-9: T568A and T568B Pin / Pair Assignments	258
Figure 9-10: Typical RFID Components	269
Figure 11-1: ICAO TRIP Strategy.....	308
Figure 12-1: Airport Stakeholder's View - Annotated.....	319
Figure 12-2: Cybersecurity Perimeter Defense.....	320
Figure D-1: A sample IDMS and Devices structure.....	D-1

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) which are hereinafter referred to as *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, as well as best practices for use by designers, manufacturers, installers, service providers, operators and users of automated integrated security systems intended for operational use within the US 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 can vary significantly from place to place. Each ASP was originally required to describe the “systems, methods or 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 PACS design.

After 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