

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
© 2013, RTCA, Inc.

Copies of this document may be obtained from

RTCA, Inc
1150 18th St. NW, Suite 909
Washington, D.C. 20036, USA

Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org

Please call RTCA for price and ordering information

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 issuance is 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 follow 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, the 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
1.1.	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.	Biometrics ConOps.....	5
1.5.4.	PACS ConOps.....	6
1.5.5.	Perimeter Intrusion Detection ConOps.....	6
1.5.6.	Video ConOps.....	7
1.5.7.	SOC ConOps.....	8
1.5.8.	Integration ConOps.....	9
1.6.	System Overview.....	9
1.6.1.	Communications.....	10
1.6.2.	Credentialing.....	10
1.6.3.	Biometrics.....	10
1.6.4.	PACS.....	11
1.6.5.	Perimeter Intrusion Detection.....	11
1.6.5.1.	Threats and Threat Vectors.....	11
1.6.6.	Video.....	13
1.6.7.	SOC.....	14
1.6.8.	Integration.....	14
1.6.8.1.	Situational Awareness.....	15
1.7.	Regulatory Requirements.....	15
1.8.	System Design.....	15
1.9.	Cyber Security.....	16
1.9.1.	National Security Initiatives.....	16
1.9.2.	FICAM Cyber Security Programs.....	16
1.9.3.	EOP-OMB Cloud Computing Initiative.....	16
1.10.	Communities of Interest.....	17

1.10.1.	Security Operations Center (SOC) Participants	17
1.10.2.	Aircraft Operators	18
1.10.3.	Federal Agencies	18
1.10.4.	LEOs	18
1.11.	Integration	19
1.11.1.	Trade Studies / Design Trade-offs.....	19
1.11.2.	Configuration Management / Interfacing / Integration / Migration Issues.....	19
2.	CREDENTIALING.....	21
2.1.	Introduction	21
2.2.	Regulatory Requirements	21
2.2.1.	Transportation Security Regulations	22
2.2.2.	U.S. Customs and Border Protection Regulations	23
2.3.	Functional Requirements.....	23
2.3.1.	Chain of Trust.....	24
2.3.2.	Identity Data Management System (IDMS).....	24
2.3.3.	Credential Applications.....	24
2.3.4.	Identity Verification	24
2.3.5.	Application Approval.....	25
2.3.6.	Enrollment.....	25
2.3.7.	Background and Security Check	25
2.3.8.	Adjudication Management	26
2.3.9.	Training Before Issuance	26
2.3.10.	Credential Issuance	26
2.3.11.	Lifecycle Credential Management	27
2.4.	Interoperability Requirements.....	28
2.4.1.	The Federal Channelers.....	28
2.4.2.	The PACS.....	29
2.4.3.	External Interfaces.....	29
2.4.4.	Breeder Document Services	29
2.5.	Credential Considerations	29
2.5.1.	Technology Trends.....	30
2.5.2.	Visible Credential Characteristics	30

2.5.3.	Privacy Issues.....	31
2.5.4.	Computer-based Training & Curriculum Delivery	31
2.5.5.	Logical Access	32
2.5.6.	Brass/Electronic Key Management	32
2.6.	References to Previous Credentialing Sections	32
3.	BIOMETRICS	35
3.1.	Introduction and Background.....	35
3.1.1.	Introduction	35
3.1.2.	Reasons to Use Biometrics.....	35
3.1.3.	Basic Functions	36
3.1.4.	Biometric Modalities.....	36
3.1.5.	Legislative and Regulatory Requirements	38
3.1.6.	Recent Technology Advances	40
3.2.	Biometric Applications	40
3.2.1.	Criminal History Records Check (CHRC).....	40
3.2.2.	De-duplication at Enrollment	41
3.2.4.	Logical Access to Security Systems.....	43
3.2.5.	ID Verification	43
3.3.	Biometric Considerations.....	44
3.3.1.	False Reject Rate (FRR).....	45
3.3.2.	False Accept Rate (FAR).....	45
3.3.3.	Equal Error Rate (EER).....	45
3.3.4.	Failure to Enroll (FTE).....	46
3.3.5.	Failure to Acquire (FTA)	46
3.3.6.	Throughput Rate.....	46
3.3.7.	Environmental Considerations	47
3.3.8.	Usability	47
3.3.9.	Anti-spoofing and Liveness Detection	48
3.4.	Enrollment Considerations	48
3.4.1.	Quality.....	48
3.4.2.	Test Verification.....	49
3.4.3.	Training (Enrollees and Operators).....	49

3.4.4.	Retention of Original Biometric Identifiers	49
3.5.	Managing Exceptions	50
3.6.	Privacy and Data Security Considerations	50
3.6.1.	Encrypted in Transit and at Rest	52
3.6.2.	Digital Signatures or other Data Protection Mechanisms	52
3.7.	Threat Vectors and Mitigation Options.....	52
3.7.1.	Sensor Spoofing	52
3.7.2.	Data Manipulation or Replacement.....	53
3.7.3.	False Identity Claim at Enrollment	53
3.7.4.	Imposter Attempts	53
3.8.	Biometric Standards	54
3.8.1.	Application Interfaces	55
3.8.2.	Data Formats	55
3.8.3.	Application Profiles.....	56
3.8.4.	Testing.....	57
3.9.	Future Biometric Trends	57
3.10.	References to Previous Biometrics Sections	58
4.	PACS	59
4.1.	Overview	59
4.2.	PACS Main Components	60
4.2.1.	Emerging PACS Technologies Cards & Readers	62
4.2.2.	Near Field Communication	62
4.2.3.	Cloud Computing in Physical Security	62
4.2.4.	Card Types	63
4.2.5.	PIN Utilization	64
4.2.6.	Credential Form Factors.....	66
4.2.7.	Card/Credential Reader Considerations	66
4.2.7.1.	Insertion and Swipe Readers	68
4.2.7.2.	Contactless and Proximity Card Readers	68
4.2.7.3.	Smart Card Reader and Data Formats	69
4.2.7.4.	Internal Exit Reader	69
4.2.8.	Portal Hardware.....	69

4.2.9.	Field Controllers.....	70
4.2.9.1.	Inter-Device Communication.....	70
4.2.9.2.	Spread Spectrum Communication.....	70
4.2.9.3.	Mutual Authentication for PACS.....	72
4.2.10.	PACS Server & Application Software: Main Functions Overview.....	72
4.2.10.1.	PACS Software.....	73
4.2.10.2.	PACS Server Hardware.....	74
4.2.10.3.	PACS Client Workstations.....	75
4.2.11.	Special PACS Use Cases.....	75
4.2.11.1.	Two Person Control.....	75
4.2.11.2.	Elevator Control.....	76
4.3.	Regulatory Requirements and Industry Standards.....	77
4.3.1.	Standards, Regulations and Guidelines Applicable to Airport Access Control Systems.....	77
4.3.1.1.	Federal Information Processing Standard (FIPS) 201.....	77
4.3.1.2.	Personal Identity Verification Interoperability for Non-Federal Issuers.....	77
4.3.1.3.	Underwriter Laboratories (UL) 294.....	78
4.3.1.4.	Underwriter Laboratories (UL) 1076.....	78
4.3.1.5.	National Fire Protection Association (NFPA).....	78
4.3.1.6.	National Electric Code (NEC).....	78
4.3.1.7.	Recommended Security Guidelines for Airport Planning, Design and Construction, TSA May, 2011.....	79
4.3.1.8.	ISO/IEC 24727 – Identification Cards – Integrated Circuit Cards Programming Interfaces [Parts 1-6].....	79
4.3.1.9.	Additional Requirements Imposed on Airport Security Systems.....	79
4.3.1.10.	Approved Products List.....	79
4.3.2.	Environmental Impact to Airport PACS.....	80
4.4.	System Design Overview (Reference ConOps).....	80
4.4.1.	Throughput at Different Boundary Areas Entry and Exit.....	80
4.4.2.	System Design Considerations - Threats.....	80
4.4.2.1.	Hardware.....	81
4.4.2.2.	Software.....	81
4.4.2.3.	Electrical.....	81
4.4.2.4.	Environmental.....	81
4.4.2.5.	Maintenance.....	82
4.5.	Portal.....	82

4.5.1.	Interior Doors	83
4.5.2.	Exterior Doors	83
4.5.3.	Fire Rated Doors	83
4.5.4.	Rotating Portals	84
4.5.5.	Mantraps	84
4.5.6.	Rollup Doors	84
4.5.7.	Vehicle Barriers.....	84
4.5.8.	Key and Lock Technologies.....	85
4.5.9.	Other.....	86
4.5.10.	Auditing and Reporting.....	86
4.5.10.1.	Server Configuration.....	87
4.5.10.2.	Power Considerations.....	88
4.6.	Authentication Mechanisms; Multiple Authentication Factors.....	88
4.6.1.	PIN-to-PACS as Single Factor Knowledge.....	90
4.6.2.	PIN-to-Card.....	91
4.6.3.	Card with PIN-to-PACS.....	91
4.6.4.	Authentication IT Infrastructure with PKI	92
4.6.5.	Operator Authentication.....	93
4.7.	PACS Technology Trends.....	95
4.7.1.	Multifactor Authentication.....	95
4.7.2.	Card – Reader Mutual Authentication.....	95
4.7.3.	Virtualization.....	95
4.8.	Interfaces with Other Systems.....	96
4.8.1.	Access Alarms.....	96
4.8.2.	Intrusion Alarms.....	97
4.8.3.	Portal Operation	97
4.8.3.1.	Portal Forced Open.....	97
4.8.3.2.	Portal Open too Long	98
4.8.3.3.	Portal Tamper.....	98
4.8.3.4.	PACS Portal Breaches & Intrusion Detection.....	98
4.8.3.5.	Integration with Video – Video assessment, Analytics, Storage and Retrieval of Event Video Clips	99
4.8.3.5.1.	Video Alarms	100
4.8.3.5.2.	Video Analytic Examples.....	100

5.	PERIMETER INTRUSION DETECTION	103
5.1.	Perimeter Intrusion Detection System Overview	103
5.1.1.	Mission.....	103
5.1.2.	Risk and Needs Assessment	104
5.2.	Regulatory Requirements	104
5.3.	Threats/Vulnerabilities	105
5.4.	Current Practices	105
5.4.1.	Fencing.....	105
5.4.2.	Sensing Technology	106
5.4.3.	Patrol	106
5.4.4.	Perimeter Maintenance.....	106
5.4.5.	Best Practices	107
5.4.6.	Perimeter Systems Product Testing.....	107
5.5.	Requirements.....	107
5.5.1.	Requirements Overview	107
5.5.2.	Requirements Traceability	108
5.5.3.	Typical PIDS Requirements	108
5.6.	System Design Considerations.....	110
5.6.1.	Design Process	110
5.6.2.	System Performance.....	110
5.6.2.1.	Performance Measures	110
5.6.2.2.	Layering of Sensing Technologies and Solutions	111
5.6.2.3.	Modeling & Simulation (M&S)	112
5.6.3.	Design Factors and Constraints.....	112
5.6.3.1.	Operational	113
5.6.3.2.	Environmental	113
5.6.3.3.	Technological.....	113
5.6.3.4.	Infrastructure Driven.....	113
5.6.4.	Tolerance for Change	114
5.6.4.1.	Maintainability and Change Management.....	114
5.6.4.2.	Adaptability	114
5.6.4.3.	Migration Plan.....	115
5.6.4.4.	Feedback Capture	115

5.7.	Industry Standards.....	115
5.8.	Current Technology.....	120
5.8.1.	Introduction	120
5.8.1.1.	Pulse Infrared (Exterior).....	125
5.8.1.2.	Coaxial Cable Technology	126
5.8.1.3.	Fiber-Optic Cable.....	126
5.8.1.4.	Underwater Fiber-optic Netting	127
5.8.1.5.	Buried Pressure Line Sensor	128
5.8.1.6.	Ported Coax Buried Cable.....	128
5.8.1.7.	Taut Wire.....	129
5.8.1.8.	Bi-static Microwave	130
5.8.1.9.	Mono-static Microwave	131
5.8.1.10.	Electric Field or Capacitance	132
5.8.1.11.	Video Motion Detection.....	133
5.8.1.12.	Thermal (LWIR) Video Analytics w/GPS Location	134
5.8.2.	Assess / Identify / Classify	135
5.8.3.	Track / Locate.....	135
5.8.3.1.	Video-Based Tracking.....	135
5.8.3.2.	Radar Systems	136
5.8.3.3.	LADAR Systems.....	137
5.8.3.4.	Geo-spatial Systems	138
5.8.4.	Other Technologies	138
5.9.	Technology Trends.....	138
5.9.1.	Wireless Technologies	138
5.9.2.	Physical Security Information Management Systems (PSIM)	139
5.10.	PIDS Integration.....	139
5.11.	Staffing, Training, and Sustainment (Maintenance).....	140
5.11.1.	Staffing Considerations	140
5.11.2.	Perimeter Training Considerations.....	140
5.11.3.	Sustainment Considerations	141
5.12.	References to Previous PIDs Sections.....	141

6.	VIDEO SURVEILLANCE SYSTEMS	143
6.1.	System Overview	143
6.2.	Video Imaging Sensors	144
6.2.1.	Selecting Cameras and Lenses	145
6.2.2.	Solid State Video Detectors	145
6.2.3.	Thermal Imaging Sensors.....	146
6.3.	Applications	147
6.3.1.	Outer Perimeter	147
6.3.2.	Landside Terminal Roadways.....	147
6.3.3.	Vehicle Access Gates	148
6.3.4.	Portals to Secured Area	149
6.3.5.	Security Checkpoints.....	150
6.4.	System Design.....	150
6.4.1.	Imager Operational Performance	151
6.4.1.1.	Performance Metrics	151
6.4.1.2.	Pixel Density Metrics	153
6.4.2.	General Architectures.....	155
6.4.3.	Open Standards	157
6.4.4.	Standards Groups	157
6.4.5.	U.S. and International Video Standards	158
6.4.6.	Security Surveillance Camera Formats	159
6.4.7.	Camera Coverage (Field-of-View).....	159
6.4.7.1.	Megapixel and HD Cameras	160
6.4.8.	Lighting.....	161
6.4.9.	Encoding.....	164
6.4.10.	Transmission	165
6.4.11.	Viewing	166
6.4.12.	Recording and Storage	168
6.4.12.1.	Storage Solutions.....	169
6.4.13.	Video Servers	171
6.4.14.	Video Analytics.....	172
6.4.15.	Video Management Systems (VMS).....	175
6.4.16.	Physical Security Information Management Systems (PSIM)	176

6.4.17.	System and Subsystem Integration.....	176
6.4.18.	Displaying Information in Command Centers	176
6.4.19.	System Testing	177
6.5.	Regulations.....	177
6.6.	Technology Trends.....	177
6.7.	Enhancing Legacy Systems with Software	179
7.	SECURITY OPERATIONS CENTER (SOC)	181
7.1.	Typical Security Operations Center	184
7.1.1.	Facilities: Standard SOC Design / Build / Operation Considerations	184
7.1.2.	Facilities: SOC Supporting PACS Communications Infrastructure.....	185
7.2.	Security Operations Center (SOC) Requirements.....	185
7.2.1.	Displaying Information in the SOC.....	186
7.3.	SOC and Situational Awareness.....	187
7.3.1.	Continuing Domain Awareness in the SOC.....	187
8.	INTEGRATION	189
8.1.	Overview	189
8.1.1.	A Value Proposition	189
8.1.2.	Integration Process	191
8.2.	Integrated System Design.....	193
8.2.1.	Integration Architecture	195
8.2.2.	Methodologies and Guides.....	196
8.2.3.	Standards	198
8.3.	Choosing a Platform.....	199
8.3.1.	Physical Security Information Management Systems (PSIM).....	200
8.4.	System Component Interoperability.....	202
8.4.1.	System Interfaces	202
8.5.	Cost Impacts.....	203
8.6.	Configuration Management / Migration Issues.....	203
8.7.	Additional Users.....	204
8.7.1.	Additional Remote Sites.....	204

9.	COMMUNICATIONS INFRASTRUCTURE.....	205
9.1.	Introduction – Overview	205
9.2.	Functional Requirements Summary	205
9.2.1.	Cellular Voice and Data	205
9.2.2.	Trunked Radio Systems and Interoperability	206
9.2.2.1.	800 MHz Trunked Radio Systems	206
9.2.2.2.	Project 25 (P25).....	206
9.2.2.3.	DHS Multiband Radios	207
9.2.3.	VHF and UHF Radios	207
9.2.4.	DHS SAFECOM Program	208
9.2.5.	Voice-over-Internet Protocol (VoIP).....	209
9.2.6.	Commercial Services.....	209
9.2.7.	Wireless IT Networks, also known as Wireless LANs (WLANs)	210
9.3.	Regulatory Requirements and Standards	210
9.3.1.	FCC Role.....	210
9.3.2.	Spectrum Considerations.....	210
9.3.3.	Communications Standards.....	212
9.4.	Threats.....	212
9.4.1.	Cybersecurity	214
9.5.	Current Practices	216
9.6.	Design Objectives	216
9.6.1.	Communications Infrastructure.....	217
9.6.2.	Network Standards	218
9.6.3.	Network Infrastructure Relationships	218
9.6.4.	Communications Functionality	220
9.7.	System Design Considerations.....	220
9.7.1.	Performance	221
9.7.2.	LAN Protocols.....	222
9.7.3.	OSI Model.....	223
9.7.4.	Topologies.....	224
9.7.5.	VLANs	225
9.7.6.	Bandwidth Management	226

9.7.7.	Quality of Service (QoS) Issues	227
9.7.8.	IP Voice.....	227
9.7.9.	Multicasting.....	228
9.7.10.	Virtual Private Network (VPN).....	229
9.8.	Network Backbone and Infrastructure	229
9.9.	Device Wiring	230
9.9.1.	Cabling Management	230
9.9.2.	Cable Plant Migration Strategy	231
9.9.3.	Wire and Cable Installation.....	231
9.9.4.	Fiber Optic Backbone Cabling.....	232
9.9.4.1.	Fiber Optic Cables and Standards	233
9.9.5.	Structured Cabling.....	233
9.9.5.1.	Structured Cabling Types and Standards	233
9.9.5.2.	Power-over-Ethernet (PoE)	237
9.9.5.3.	Color Codes for RJ-45 Ethernet Plug and Jack.....	237
9.9.5.4.	Performance Verification and Testing	238
9.9.6.	End Point Connections	239
9.9.7.	Complying with Standards	240
9.9.8.	Labeling.....	240
9.9.9.	Telecommunication Rooms (TRs)	241
9.10.	Wireless Networks and Devices.....	242
9.10.1.	Wireless Communications.....	242
9.10.2.	Wireless LANs	242
9.10.3.	WiFi Wireless LANs.....	245
9.10.4.	WiMAX.....	246
9.10.5.	Long Range WiFi Communications.....	246
9.10.6.	Radio Frequency Identification (RFID)	247
9.10.7.	Near-Field Communications (NFC).....	248
9.10.8.	Radio over IP (RoIP).....	248
9.11.	Privacy and Data Security Considerations	249
9.11.1.	Network Security Standards and Guidelines.....	249
9.11.2.	Transmission and Data Security.....	250
9.11.3.	Network Security.....	250
9.11.3.1.	Establishing Network Security.....	251

9.11.3.2.	Public Key Infrastructures (PKIs)	253
10.	GENERAL ACQUISITION RELATED CONSIDERATIONS	255
10.1.	Introduction	255
10.2.	Regulatory Requirements	255
10.2.1.	Federal, State, and Local Regulatory Requirements	255
10.2.1.1.	49 Code of Federal Regulation Part 1542, Airport Security	255
10.2.1.2.	Federal Security Guidelines	256
10.2.1.3.	Disclosure of Security Sensitive Information (SSI)	256
10.3.	System Acquisition Phase	257
10.3.1.	System Design.....	257
10.3.2.	System Design Objectives.....	257
10.3.2.1.	Standards-Based Open Architecture	258
10.3.2.2.	Interoperability	258
10.3.2.3.	Scalability.....	258
10.3.2.4.	Reliability, Maintainability, and Availability.....	258
10.3.3.	Legacy System Integration.....	259
10.3.4.	System Specification and Selection	259
10.4.	System Installation Phase.....	260
10.5.	Implementation Phasing Considerations	261
10.6.	System Documentation	261
10.6.1.	As-Built Drawings and Bill of Materials	261
10.6.2.	Operational Procedures Format and Content	261
10.7.	Training Manuals and Courses.....	261
10.7.1.	ISSA Operator Training	262
10.7.2.	Systems Administrator Training	262
10.7.3.	Maintenance Training	263
10.7.4.	Biometrics – Special User Training Considerations	263
10.8.	System Test, Verification and Validation	263
10.8.1.	System Test	264
10.8.1.1.	System Test Plan Development.....	264
10.8.1.1.1.	Testing of Revisions or Upgrades	265
10.8.1.2.	System Test Procedure Development.....	265

10.8.1.3.	System Qualification and Acceptance Testing.....	266
10.8.1.4.	Site Installation Testing.....	266
10.8.1.5.	Operational Transition Plan.....	266
10.8.1.6.	Operational Testing	267
10.8.1.7.	Sample Test Plan.....	267
10.8.2.	Special Biometric Subsystem Testing and Certification	267
10.9.	Warranty Requirements.....	267
10.10.	System Logistics Support.....	268
10.10.1.	Maintenance Considerations	268
11.	MEMBERSHIP	271
APPENDIX A STANDARDS.....		A-1
A.1	FEDERAL, STATE, AND LOCAL	A-2
A.1.1.1	CODE OF FEDERAL REGULATIONS (CFR) [WWW.EFCR.GOV].....	A-2
A.1.1.2	TRANSPORTATION SECURITY ADMINISTRATION (TSA) [WWW.TSA.GOV].....	A-2
A.1.1.3	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) [WWW.NIST.GOV]	A-2
A.1.1.4	DEPARTMENT OF DEFENSE (DOD) [WWW.DOD.GOV]	A-2
A.1.1.5	OTHER AGENCIES	A-2
A.1.2	INDUSTRY AND INTERNATIONAL STANDARDS [WWW.ANSI.ORG]	A-3
A.1.2.1	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE) [WWW.IEEE.ORG].....	A-3
A.1.2.3	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) [WWW.ISO.ORG]	A-3
A.1.2.4	NATIONAL ELECTRICAL MANUFACTURERS ASSOCIATION (NEMA) [WWW.NEMA.ORG]....	A-4
A.1.2.5	NATIONAL FIRE PROTECTION ASSOCIATION (NFPA) [WWW.NFPA.ORG]	A-4
A.1.2.6	UNDERWRITERS' LABORATORIES (UL) [WWW.UL.COM].....	A-4
APPENDIX B:	GLOSSARY	B-1
APPENDIX C	REFERENCES	C-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) 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