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

Standards for
Airport Security Access Control Systems

RTCA DO-230M
March 14, 2024

Prepared by: SC-224
© 2024 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 March 14, 2024.

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 the basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration (FAA) Technical Standard Orders and several advisory circulars.

All URLs referenced in this document are current as of the document publication date.

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.

EXECUTIVE SUMMARY

The RTCA document DO-230M provides guidance on acquiring and designing Airport Security Access Control Systems, as well as the integration, testing, system performance evaluation, and operational requirements related to such access control systems.

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, physical access control system, security operations center, video surveillance, cybersecurity, and communications sections with minor changes throughout other sections of the document. Advances in biometrics technology, artificial intelligence (AI), neural networks, and facial recognition coupled with evolving cybersecurity threats and vulnerabilities have been included in this release.

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, enhanced biometric credentials, inspections for credential holders, updates to REAL IP, enhanced cybersecurity controls for credentialing systems and guidance on privacy protection based on the increased amount of personal identifiable information that is collected for the issuance of credentials. Visitor vetting and enhancements to the credential issuance programs were also included in this update. For readers of this 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 potential impacts to their credentialing and airport access policies.

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. Airport operators should take necessary steps to stay updated with cybersecurity vulnerabilities that are published by the Department of Homeland Security (DHS) Cybersecurity Infrastructure Security Agency (CISA) and other government and industry organizations. CISA's focus goes beyond information technology equipment and includes industrial control systems (HVAC, Lighting, Fuel Depot, etc.) that are becoming increasing vulnerable to cybersecurity threats and airport operators should be concerned beyond the access control systems. The NIST Special Publication (SP) 800-53 Revision 5 was finalized since the last release of DO-230 and updates to the Credentialing, Biometrics, physical access control system, communications, and video surveillance sections were included in this relace to provide guidance to airport operators on applicable security controls.

The nature of video surveillance equipment changes due to technological enhancements/obsolescence 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 and video management 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 Transportation Security Administration (TSA), airports, and industry representatives for inclusion in the revised credentialing section.

While the Federal Aviation Administration (FAA) Reauthorization Act of 2012 requires 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.

Notwithstanding, drone/UAV captured images of airports, especially special-use and joint military/civilian airports may be federally classified as Sensitive Security 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 DHS Privacy Office continues to provide publications on topics such as border security, cybersecurity, transportation security on their website.

This RTCA DO-230M 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.

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 assorted 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 5
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
1.5.9 Threats and Threat Vectors 8
1.6 System Overview 10
1.6.1 Communications 11
1.6.2 Credentialing 11
1.6.3 Biometrics 11
1.6.4 PACS 11
1.6.5 Perimeter Intrusion Detection 12
1.6.6 Video 12
1.7 SOC 12
1.7.1 SOC Participants 13
1.7.2 Aircraft Operators 14
1.7.3 Federal Agencies 15
1.7.4 LEOs 15
1.7.5 Incident Response Posts 15
1.8 Integration 15
1.8.1 Trade Studies / Design Trade Offs 16
1.8.2 Configuration Management / Interfacing / Integration / Migration Issues 16
1.8.3 Situational Awareness 16
1.9 Communications 17
1.10 General Acquisition-Related Considerations 17
1.11 Facilitation 17
1.11.1 Standards, Regulatory Requirements and Recommended Practices 17
1.11.2 National Security Initiatives 18
1.11.3 EOP-OMB Cloud Computing Initiative 18
1.12 Cybersecurity 19
1.12.1 FICAM Cyber Security Programs 19

2 CREDENTIALING 21

2.1 Introduction and Purpose 21
2.2 Federally Regulated Credentialing Process 23
2.2.1 Application Process 23

2.2.2 Identify Verification Process 24
2.2.3 Background and Security Check Process 25
2.2.4 Adjudication Management Process 25
2.2.5 Training Function 27
2.2.6 Credential Issuance Process 28
2.2.7 Lifecycle Credential Management 28
2.2.8 Credential Regulatory / Compliance Requirements 29
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 32
2.3.3 Fully Automated Management Systems (IDMS) 33
2.4 Contrasting Automation Approaches 33
2.5 Cybersecurity in Credentialing 34
2.6 Credentialing Trends 35
2.6.1 Next Generation Identification (NGI) 35
2.6.2 Enhanced Criminal History Checks 36
2.6.3 Biometric Enhanced Credentials 36
2.6.4 REAL ID 36
2.6.5 Inspection of Credential Holders 36
2.6.6 Privacy Protection 37
2.6.7 Customs and Border Protection (CBP) eBadge Trusted Worker Program (TWP) 37
2.6.8 Visitor Vetting and Credential Issuance Programs 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 46
3.2.3 Physical Access Control 47
3.2.4 Logical Access to Security Systems 49
3.2.5 ID Verification 49
3.3 Biometric Considerations 50
3.3.1 False Rejection Rate (FRR) 51
3.3.2 False Acceptance Rate (FAR) 51
3.3.3 Equal Error Rate (EER) 52
3.3.4 Failure to Enroll (FTE) 52
3.3.5 Failure to Acquire (FTA) 52
3.3.6 Throughput Rate 53
3.3.7 Environmental Conditions 53

3.3.8 Usability 54
3.3.9 Anti-spoofing and Liveness Detection 54
3.4 Enrollment Considerations 54
3.4.1 Quality 54
3.4.2 Test Verification 55
3.4.3 Training (Enrollees and Operators) 55
3.4.4 Retention of Original Biometric Identifiers 56
3.5 Managing Exceptions 56
3.6 Privacy and Data Security Considerations 56
3.6.1 Encrypted in Transit and at Rest 58
3.6.2 Digital Signatures or other Data Protection mechanisms 58
3.7 Threat Vectors and Mitigation Options 59
3.7.1 Sensor Spoofing 59
3.7.2 Data Manipulation or Replacement 59
3.7.3 False Identity Claim at Enrollment 59
3.7.4 Imposter Attempts 60
3.8 Biometric Standards 60
3.8.1 Technical Interfaces 62
3.8.2 Data Formats 63
3.8.3 Implementations 64
3.8.4 Testing and Reporting 65
3.8.5 Status of National and International Biometric Standards Projects 66
3.9 Future Biometric trends 71
3.10 Biometrics Checklist 72

4 PHYSICAL ACCESS CONTROL SYSTEM (PACS) 75

4.1 Overview 75
4.2 PACS Main Components 75
4.2.1 Emerging PACS Technologies – Cards and Readers 77
4.2.2 Near Field Communication (NFC) 77
4.2.3 Cloud Computing in Physical Security 77
4.2.4 Card Types 78
4.2.5 Personal Identification Number (PIN) Utilization 80
4.2.6 Card Technologies 81
4.2.7 Card/Credential Reader Considerations 82
4.2.8 Portal Door Hardware 85
4.2.9 Field Controllers 85
4.2.10 PACS Server & Application Software: main Functions Overview 88
4.2.11 Special PACS Use Cases 91
4.3 Regulatory Requirements and Industry Standards 93
4.3.1 Standards, Regulations and Guidelines Applicable to Airport ACS 93
4.3.2 Environmental Impact to Airport PACS 96
4.4 System Design Issues Overview (Reference ConOps) 96
4.4.1 Throughput at Different Boundary Areas Entry and Exit 96
4.4.2 System Design Considerations – Threats 97
4.4.3 Hardware 97
4.4.4 Software 97
4.4.5 Electrical 97
4.4.6 Environmental 98

4.4.7 Maintenance ... 98
4.5 Portal Operation ... 98
4.5.1 Portal Position Switch ... 98
4.5.2 Interior Doors ... 99
4.5.3 Exterior Doors ... 99
4.5.4 Fire Rated Doors ... 99
4.5.5 Automated Exit Lane Breach Control ... 100
4.5.6 Rotating Portals ... 104
4.5.7 Mantraps ... 104
4.5.8 Rollup Doors ... 104
4.5.9 Vehicle Barriers ... 104
4.5.10 Key and Lock Technologies ... 105
4.5.11 Other ... 106
4.5.12 Auditing and Reporting ... 106
4.5.13 Server Configuration ... 106
4.5.14 Power Considerations ... 107
4.6 Authentication Mechanisms; Multiple Authentication and Security Factors ... 108
4.6.1 PIN-to-PACS as Single Factor Knowledge ... 110
4.6.2 PIN-to-Card Operation ... 110
4.6.3 Card with PIN-to-PACS Operation ... 111
4.6.4 Authentication IT Infrastructure with PKI ... 112
4.6.5 PACS System Operator Authentication ... 113
4.6.6 Data Protection: Data in Transit ... 113
4.7 PACS Technology Trends ... 114
4.7.1 Multifactor Authentication, Stand Alone, Self-Contained Reader ... 114
4.7.2 Card-Reader Mutual Authentication ... 115
4.7.3 Virtualization ... 116
4.8 Interfaces with Other Systems ... 116
4.8.1 Access Alarms ... 117
4.8.2 Intrusion Alarms ... 117
4.8.3 Portal Operations ... 117
4.9 Pilot Access ... 121
4.10 Mobile ID Credential in Airport Access Control ... 122
4.10.1 Trusted Framework for Identity Vetting, Mobile Device Registration, Credential Creation and Download ... 122
4.10.2 Airport Passengers and Employees ... 123
4.10.3 Multifactor Authentication ... 123
4.10.4 Mobile ID Credential in Airport Access Control Summary ... 124
4.11 Physical Access Control System (PACS) Checklist ... 124

5 PERIMETER INTRUSION DETECTION ... 129

5.1 Introduction ... 129
5.2 Perimeter Intrusion Detection System Overview ... 129
5.2.1 PIDS Definition ... 129
5.2.2 Perimeter Security Risks ... 130
5.2.3 PIDS Security Objectives ... 130
5.3 Code and Regulatory Requirements ... 131
5.3.1 TSA ... 131
5.3.2 FAA ... 132

5.3.3 ICAO 132
5.3.4 Industry Standards 132
5.4 PIDS Requirements 132
5.4.1 Assessment of Threats and Vulnerabilities 132
5.4.2 Requirements Overview 133
5.5 Perimeter Security 136
5.5.1 Physical Elements 137
5.5.2 Technology-based Elements 137
5.5.3 Integration/Coordination with Other Security Systems 153
5.5.4 Operational and Procedural Elements 156
5.6 PIDS Implementation 158
5.7 System Design Considerations 159
5.7.1 Design Process 159
5.7.2 System Performance 159
5.7.3 Design Factors and Constraints 162
5.8 References to Previous PIDS Sections 164
5.9 Industry Standards 164
5.10 Commercial Security Guideline References 168
5.11 Military and Nuclear Security Guideline References 168
5.12 Perimeter Intrusion Detection Checklist 170

6 VIDEO SURVEILLANCE SYSTEMS 171

6.1 System Overview 171
6.2 Application of VSS 172
6.2.1 Alarm Monitoring and Assessment 172
6.2.2 Perimeter and Surveillance 174
6.2.3 Forensic Review 175
6.2.4 Integration with Other Systems 175
6.3 Design Considerations 176
6.3.1 VSS Design 177
6.3.2 Imager Operational Performance 178
6.3.3 Imaging Sensor Type 179
6.4 VSS Architecture 179
6.4.1 Video Management Systems (VMS) 181
6.4.2 Clients 182
6.4.3 Video Recording Servers 183
6.4.4 Storage 184
6.4.5 Cameras 187
6.4.6 Microphones 195
6.5 Video Analytics 195
6.5.1 Applications 196
6.5.2 Edge-based Analytics 198
6.5.3 Server-based Analytics 198
6.5.4 Cloud-based Analytics 198
6.5.5 Artificial Intelligence 198
6.6 Lighting 199
6.7 Information Technology (IT) and Network Considerations 201
6.7.1 Bandwidth Utilization 202
6.7.2 VLANs and Firewalls 203

6.7.3 Cybersecurity considerations 203
6.7.4 Virtualization 204
6.8 Standards 204
6.8.1 Open Standards 204
6.8.2 Standards Groups 205
6.8.3 Networking Standards 206
6.8.4 U.S. and International Video Standards 206
6.8.5 Encoding 207
6.9 Regulations 208
6.10 System Testing 208
6.10.1 Performance Metrics 208
6.10.2 Analytics Testing 209
6.11 Technology Trends 209
6.12 Video Surveillance Checklist 211

7 SECURITY OPERATIONS CENTER (SOC) 213

7.1 Typical SOC 216
7.1.1 Facilities: Standard SOC Design / Build / Operation Considerations 216
7.1.2 Facilities: SOC Supporting PACS Communications Infrastructure 217
7.2 SOC Requirements 217
7.2.1 Displaying Information in the SOC 218
7.3 SOC and Situational Awareness 218
7.3.1 Continuing Domain Awareness in the SOC 219
7.4 SOC Checklist 220

8 INTEGRATION 221

8.1 Overview 221
8.2 Analysis of the Airport's Needs 221
8.2.1 Current Requirements 221
8.2.2 Future Requirements 222
8.2.3 Gap Analysis 222
8.3 Integration Strategy 223
8.3.1 Overview 223
8.3.2 Designing the Target Architecture 223
8.3.3 Priority Setting & Delivery Sequencing 227
8.4 Integration Trends 228
8.5 Planning Tips 228
8.6 Integration Checklist 229

9 COMMUNICATIONS & INFORMATION TECHNOLOGY (IT) 231

9.1 Introduction – Overview 231
9.2 System Requirements for Access Control 233
9.2.1 Communications Infrastructure 233
9.3 Wired Communication Systems 234
9.3.1 Telephone Systems 234
9.4 Wireless Communications Systems 235
9.4.1 Spectrum Considerations 235

9.4.2 FCC Role 236
9.4.3 Common Carrier Cellular Services 237
9.4.4 Special Wireless Services 239
9.4.5 Trunked RF Systems 239
9.4.6 DHS Multiband Radios 240
9.4.7 VHF and UHF Radios 241
9.4.8 DHS SAFECOM Program and CISA 241
9.4.9 Commercial Services 242
9.5 Wired and Wireless Networks 243
9.5.1 Network Infrastructure Relationships 243
9.5.2 Communications Functionality 243
9.5.3 Zero Trust Network (ZTN) 244
9.5.4 Network Design Considerations 245
9.5.5 Network Standards 248
9.5.6 Network Monitoring and Management 255
9.6 Network Backbone and Infrastructure 255
9.6.1 End Point Connections 256
9.6.2 Passive Optical Network (PON) 257
9.6.3 Cabling and Cable Management 257
9.6.4 Fiber Optic Cabling 260
9.7 Structured Cabling 263
9.7.1 Structured Cabling Types and Standards 264
9.7.2 Performance Verification and Testing 266
9.7.3 Complying with Standards 266
9.8 Telecommunication Rooms (TRs) 267
9.9 Wireless Networks and Devices 268
9.9.1 Wireless Communications 268
9.9.2 Wireless LANs (WLAN) 269
9.9.3 Optical (Laser) Communications 270
9.9.4 Regulatory Requirements and Standards 270
9.9.5 Wi-Fi 802.11 Wireless Standards 271
9.9.6 WiMAX 273
9.9.7 Long Range Wi-Fi Communications 273
9.9.8 Radio Frequency Identification (RFID) 274
9.9.9 Near-Field Communications (NFC) 275
9.9.10 Radio over IP (RoIP) 275
9.10 Privacy and Data Security Considerations 276
9.10.1 The General Data Protection Regulation (2016/679, (GDPR) 277
9.10.2 Transmission and Data Security 277
9.11 Network Security 277
9.11.1 NIST Cybersecurity Standards 278
9.11.2 ISA Security Standards 279
9.11.3 Threats and Vulnerabilities 279
9.12 Designing a Secure Network 281
9.12.1 Public Key Infrastructures (PKIs) 283
9.13 Trends 284

10 GENERAL ACQUISITION-RELATED CONSIDERATIONS 287

10.1 Introduction 287
10.2 Airport Needs Assessment 287
10.2.1 Assess Current Capabilities and Systems 287
10.2.2 Gap Analysis 287
10.2.3 Identify Target Outcomes 288
10.3 Procurement Strategy 288
10.3.1 Considerations 288
10.3.2 Options 289
10.3.3 Best Practices 290
10.4 Funding Acquisition 291
10.4.1 Assessment 291
10.4.2 Source (Local, State & Federal) 292
10.4.3 Business Case 292
10.5 Procurements Execution 292
10.5.1 Scope Preparation 293
10.5.2 Disclosure of Sensitive Security Information (SSI) 294
10.5.3 Proposal Assessment 294
10.5.4 Provider Selection 294
10.5.5 Contract Negotiations 295
10.6 System Design 295
10.6.1 Guiding Principals 296
10.7 System Installation 298
10.7.1 Implementation Phasing Considerations 298
10.7.2 Preparation and Installation 298
10.7.3 Migration and Cutover 299
10.8 Testing and Acceptance Considerations 299
10.8.1 Test Strategy 299
10.8.2 System Test Development 300
10.8.3 System Test Procedure Development (STProc) 301
10.8.4 Test Execution 301
10.9 Training Courses 303
10.9.1 ISSA Operator Training 303
10.9.2 Systems Administrator Training 304
10.9.3 Maintenance Training 304
10.10 System Documentation 304
10.10.1 As-Built Drawings & Bill of Materials 304
10.10.2 Operational Procedures Format and Content 305
10.10.3 Training Manuals 305
10.11 Warranty & Maintenance 305
10.11.1 Warranty Requirements 305
10.11.2 System Logistics 305
10.11.3 Maintenance Considerations 305
10.12 Procurement Checklist 306

11 FACILITATION 309

11.1 Preface 309
11.2 History / Background 310
11.3 Major Elements of International Arrival Facilities 311
11.3.1 International Arrivals Facilities—Federal Inspection Services 311
11.3.2 CCTV 311
11.3.3 CBP Primary Inspection 311
11.3.4 Baggage Claim 312
11.3.5 CBP Secondary Inspection and Processing 312
11.3.6 Transfer Passenger Re-Check 312
11.3.7 Meeter/Greeter Lobby 312
11.3.8 CBP Administrative and Support Areas 312
’ 313
11.4 Technical Specifications 313
11.4.1 Power and Capacity: 314
11.4.2 Baggage Handling Systems (BHS): 314
11.4.3 Intrusion Detection System (IDS) 314
11.5 Recent Regulatory and Operational Changes and Initiatives: 315
11.6 Anticipated Future Requirements: 316
11.7 Operational Realities: 317
11.8 Technical Advances 318
11.9 Newly Identified Best Practices 319
11.10 Standards, Regulatory Requirements & Recommended Practices 319

12 CYBERSECURITY 321

12.1 Introduction 321
12.2 Types of Threats 321
12.3 Layered Approach to Cybersecurity 322
12.4 NIST Cybersecurity Framework 325
12.5 ICAO Aviation Cybersecurity 326
12.6 CANSO Cybersecurity 327
12.7 Zero Trust Architecture 328
12.8 Conclusion 329

13 MEMBERSHIP 333

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 – IDENTITY 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

ANNEX 4-1 CONSIDERATIONS FOR INTEROPERABLE IDENTITY & ACCESS CREDENTIAL 125

ANNEX 4-2 NON-STANDARD APPLICATION OF ACCESS CREDENTIAL 128

TABLE OF TABLES

Table 1-1: Airport Security Areas of Concern, Threats, and Countermeasures 9

Table 4-1: PACS Standard Components 76
Table 4-2: Contactless Smart Card vs. Proximity Card Technologies 79
Table 4-3: PACS & Level of Assurance 80

Table 5-1: Example of Key Performance Parameters 160
Table 5-2: System Type – Sensor Technology Pd Comparison 161
Table 5-3: Typical PIDS-Related Standards 165

Table 6-1: Redundant Array of Independent Disks (RAID) Levels 186
Table 6-2: Common Camera Types and Their Pixel Counts 188
Table 6-3: Angular and Linear Field Coverage for Camera-Lens Combinations 193
Table 6-4: Typical Illumination Standards 200

Table 9-1: Fiber Type vs. Speed and Distances 261
Table 9-2: Color Coding of Optical Fiber Cabling 261
Table 9-3: TIA Cable Classifications and Standards 264
Table 9-4: Comparison of Mobile Access Methods 268
Table 9-5: Wi-Fi 802.11 Wireless Standards Generations 271
Table 9-6: Characteristics of IEEE WLAN Standards 272

Table 12-1: Families of Controls 326

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 22

Figure 3-1: Generic Biometric Processes 48

Figure 4-1: Sample PACS Configuration 76
Figure 4-2: Sample PACS and IDMS Components 77
Figure 4-3: Cards and Card Data – Current Industry Trends 81
Figure 4-4: Physical Access Control Form Factors 82
Figure 4-5: Typical Master Key Schema 105
Figure 4-6: Reader to Controller Data Flow 110
Figure 4-7: Generic PKI-Enabled PACS Configuration 112
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) 114

Figure 5-1: Typical PIDS Progression 130

Figure 6-1: Components and Generic Architecture of a VSS 172
Figure 6-2: Determining Pixel per Foot (PPF) Values 191
Figure 6-3: Camera Angular Coverage and Typical Performance Values 194

Figure 7-1: Typical SOC Information Flow Diagram 215
Figure 7-2: Examples of SOC Configurations – Small / Medium / Large 218

Figure 9-1: Typical Communications & IT Security Functions 231
Figure 9-2: Typical Airport Communications & IT Security Logical Interfaces 232
Figure 9-3: ConOps Functional Relationships 233
Figure 9-4: Spectrum Band and Frequency Assignment 235
Figure 9-5: Spread-Spectrum Signals 236
Figure 9-6: Frequency Band Allocations 240
Figure 9-7: Communication Relationship 243
Figure 9-8: Network Communication Services 244
Figure 9-9: IEEE 802 Series Standards 249
Figure 9-10: OSI Stack 250
Figure 9-11: Network Topologies 251
Figure 9-12: Common Wide Area Network Elements Configured for Redundancy 252
Figure 9-13: Example of Network Elements Configured for Redundancy 253
Figure 9-14: Cross Sections of SMF and MMF Cables 260
Figure 9-15: WDM Block Diagram 263
Figure 9-16: T568B and T568A Pin / Pair Assignments 265
Figure 9-17: Typical RFID Components 274
Figure 9-18: Elements of the NIST Cybersecurity Framework 278
Figure 9-19: PKI Authentication Relationships 283

Figure 12-1: Airport Stakeholder's View - Annotated 323
Figure 12-2: Cybersecurity Perimeter Defense 324

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 U.S. National Airspace System (NAS) and include industry best practices and lessons learned by industry subject matter experts. Guidance provided outside of staff access control areas in this section should only be considered informative in nature.

1.2 History

In 1973, the U.S. 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 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 updated version of FAR 107 was issued, with mostly 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

 © 2024 RTCA, Inc.

few significant changes, to *Code of Federal Regulations (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 the PACS design provisions remained mostly unchanged, details of their implementation and operation have been modified regularly since, primarily by improvements in technology as well as TSA-issued Security Directives (SDs) and ASP amendments that modify performance requirements.

Various other initiatives have also provided input to this document. These include the:

- Various findings studied by TSA have influenced other standards bodies such as NIST, ISO/IEC and ICAO [Refer to Appendix A - Standards].
- National Safe Skies Alliance commitment to airport operators and facilities, technology providers and government organizations through its testing facilities, product research and lifecycle analysis of devices and systems, and their Program for Applied Research in Airport Security (PARAS).
- "Personal Identity Verification" (PIV) Program and associated standards (*FIPS 201- Federal Information Processing Standard 201)* issued by NIST in 2006 and numerous supporting documents since (including *FIPS 201-2 July 2012).*

1.3 Scope

The standards outlined herein establish application recommendations for components, processes, methods, designs, and engineering practices in the implementation of ISSA systems. In addition, the document contains significant additional material on potential extensions of such systems over and above the current regulatory requirements in line with industry practice, anticipated regulatory requirements and new technology. It contains explicit material on system migration issues. This document includes criteria deemed appropriate to standards intended to achieve the highest practical degree of commonality of interfaces between system or subsystem hardware and software modules and interchangeability of these modules across a wide range of products and manufacturers.

These performance standards do not replace technical specifications that must be developed by end users to tailor ISSA requirements to specific purposes such as system acquisition, installation, operation, training, and maintenance.

These standards provide the foundation upon which such ISSA technical specifications should be developed. The operational goals are the installation and/or implementation of an FAA- and TSA-approved ISSA that enables an airport operator to comply with the regulatory requirements, to minimize costs and operational impacts, to maximize utility for operational users, and to provide a sound foundation for the support of anticipated new requirements, technology, and standards.

1.4 Methodology

ISSA (colloquially referred to Access Control Systems (ACS)) should reflect the security strategy for an entire airport operation; its planning should take into consideration.

- Who are the stakeholders of the system(s)?
- What access control technologies exist?
- What are the migration, obsolescence, and/or emerging technology strategies?
- When is the implementation planned for the system (considering migration and obsolescence issues)?
- Where are the funding sources for the system?

Access control policies need to be developed (or enhanced and modified) to address current and emerging stakeholder needs and technological changes that could change how some policies are implemented. These policies may determine what software systems or