

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

**Standards for  
Airport Security Access Control  
Systems**

RTCA DO-230J  
December 19, 2019

Prepared by SC-224  
©2019 RTCA, Inc.

Copies of this document may be obtained from

RTCA, Inc.

Telephone: 202-833-9339

Facsimile: 202-833-9434

Internet: [www.rtca.org](http://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 December 19, 2019.

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; 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.

## 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, communications, credentialing, physical access control system, and video surveillance sections and minor changes throughout other sections of the document. 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 physical access control section was updated to add suggested guidance on how to address the issue of general aviation (GA) pilots at commercial airports and the credentialing process for unescorted access. The area of cyber security continues to evolve at a rapid pace and this section of the communications chapter is slated for updates in a future release of DO-230 as it pertains to guidance to airport operators.

For readers of the credentialing section, the National Institute of Standards and Technology (NIST) released 800-63 to address policy changes in identity management. The guidance pertains to Federal Government users and while not applicable to airport operators, RTCS 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.

As in previous releases of DO-230, Special Committee 224 (SC-224) received input from the TSA, airports, and industry representatives for revision 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 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.

This RTCA DO-230J 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.

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). As in previous releases of this document, RTCA SC- 224 recommends that readers of this guidance document solicit the Cloud information from service providers.

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 (American Association of Airport Executives (AAAE), 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 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 differences should in no way detract from the substance of the subject matter contained within the individual chapters.

## TABLE OF CONTENTS

<b>1.</b>	<b>INTRODUCTION</b> .....	<b>1</b>
<b>1.1.</b>	<b>Purpose</b> .....	<b>1</b>
<b>1.2.</b>	<b>History</b> .....	<b>1</b>
<b>1.3.</b>	<b>Scope</b> .....	<b>2</b>
<b>1.4.</b>	<b>Methodology</b> .....	<b>2</b>
<b>1.5.</b>	<b>High-Level Concept of Operations (ConOps)</b> .....	<b>3</b>
1.5.1.	Communications ConOps.....	4
1.5.2.	Credentialing ConOps.....	4
1.5.3.	Biometrics 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
<b>1.6.</b>	<b>System Overview</b> .....	<b>8</b>
1.6.1.	Communications.....	9
1.6.2.	Credentialing.....	9
1.6.3.	Biometrics.....	9
1.6.4.	PACS.....	10
1.6.5.	Perimeter Intrusion Detection.....	10
1.6.5.1.	Threats and Threat Vectors.....	10
1.6.6.	Video.....	12
1.6.7.	SOC.....	12
1.6.8.	Integration.....	13
1.6.8.1.	Situational Awareness.....	13
<b>1.7.</b>	<b>Standards, Regulatory Requirements and Recommended Practices</b> .....	<b>14</b>
<b>1.8.</b>	<b>Cyber Security</b> .....	<b>15</b>
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.....	15
1.8.5.	Aircraft Operators.....	17

1.8.6.	Federal Agencies.....	17
1.8.7.	LEOs .....	17
1.8.8.	Incident Response Posts.....	17
<b>1.9.</b>	<b>Integration.....</b>	<b>18</b>
1.9.1.	Trade Studies / Design Trade-offs .....	18
1.9.2.	Configuration Management / Interfacing / Integration / Migration Issues .....	18
<b>2.</b>	<b>CREDENTIALING.....</b>	<b>19</b>
<b>2.1.</b>	<b>Introduction and Purpose.....</b>	<b>19</b>
<b>2.2.</b>	<b>Federally Regulated Credentialing Processes.....</b>	<b>21</b>
2.2.1.	Application Process .....	21
2.2.2.	Identity Verification Process.....	22
2.2.3.	Background and Security Check Process.....	22
2.2.4.	Adjudication Management Process.....	23
2.2.4.1.	Rap Back.....	24
2.2.5.	Training Function.....	25
2.2.6.	Credential Issuance Process.....	25
2.2.7.	Lifecycle Credential Management.....	25
2.2.7.1.	New Credential .....	26
2.2.7.2.	Renewal .....	26
2.2.7.3.	Replacement.....	26
2.2.7.4.	Revocation .....	26
2.2.8.	Credential Regulatory Compliance Requirement .....	27
2.2.9.	Other Function .....	27
2.2.10.	Typical Credentialing System Interfaces .....	27
2.2.10.1.	Designated Aviation Channeler (DAC).....	28
2.2.10.2.	Physical Access Control System (PACS).....	28
2.2.10.3.	Fingerprint Capture.....	28
2.2.10.4.	Computer Based Training (CBT).....	28
2.2.10.5.	Reference Biometrics Reader .....	29
2.2.10.6.	Document Scanners .....	29
2.2.10.7.	Electronic Signature Pad Systems .....	29
<b>2.3.</b>	<b>Credential Implementation Systems.....</b>	<b>29</b>
2.3.1.	Manually Managed Credentialing Systems .....	29
2.3.2.	Partially Integrated Based on Existing Computer PACS.....	30

2.3.3.	Fully Automated Identity Management Systems (IDMS) .....	30
<b>2.4.</b>	<b>Contrasting Automation Approaches .....</b>	<b>31</b>
<b>2.5.</b>	<b>Cybersecurity in Credentialing .....</b>	<b>32</b>
<b>2.6.</b>	<b>Credentialing Trends .....</b>	<b>33</b>
2.6.1.	Next Generation Identification (NGI) .....	33
2.6.2.	Enhanced Criminal History Checks .....	33
2.6.3.	FIPS 201 .....	33
2.6.4.	REAL ID .....	34
2.6.5.	Inspection of Credential Holders .....	34
2.6.6.	Enhanced Oversight Activities .....	34
<b>2.7.</b>	<b>Credentialing Implementation Checklist .....</b>	<b>35</b>
<b>2.8.</b>	<b>Credentialing Operational Checklist .....</b>	<b>35</b>
<b>3.</b>	<b>BIOMETRICS .....</b>	<b>39</b>
<b>3.1.</b>	<b>Introduction and Background .....</b>	<b>39</b>
3.1.1.	Introduction .....	39
3.1.2.	Reasons to Use Biometrics .....	39
3.1.3.	Basic Functions .....	40
3.1.4.	Biometric Modalities .....	40
3.1.5.	Legislative and Regulatory Requirements .....	42
3.1.6.	Recent Technology Advances .....	43
<b>3.2.</b>	<b>Biometric Applications .....</b>	<b>44</b>
3.2.1.	Criminal History Records Check (CHRC) .....	44
3.2.2.	De-duplication at Enrollment .....	44
3.2.3.	Physical Access Control .....	45
3.2.4.	Logical Access to Security Systems .....	47
3.2.5.	ID Verification .....	47
<b>3.3.</b>	<b>Biometric Considerations .....</b>	<b>48</b>
3.3.1.	False Reject Rate (FRR) .....	49
3.3.2.	False Accept Rate (FAR) .....	49
3.3.3.	Equal Error Rate (EER) .....	49
3.3.4.	Failure to Enroll (FTE) .....	50
3.3.5.	Failure to Acquire (FTA) .....	50
3.3.6.	Throughput Rate .....	50
3.3.7.	Environmental Considerations .....	51

3.3.8.	Usability.....	51
3.3.9.	Anti-spoofing and Liveness Detection.....	52
<b>3.4.</b>	<b>Enrollment Considerations.....</b>	<b>52</b>
3.4.1.	Quality .....	52
3.4.2.	Test Verification .....	52
3.4.3.	Training (Enrollees and Operators).....	53
3.4.4.	Retention of Original Biometric Identifiers .....	53
<b>3.5.</b>	<b>Managing Exceptions .....</b>	<b>53</b>
<b>3.6.</b>	<b>Privacy and Data Security Considerations.....</b>	<b>54</b>
3.6.1.	Encrypted in Transit and at Rest .....	55
3.6.2.	Digital Signatures or other Data Protection Mechanisms .....	56
<b>3.7.</b>	<b>Threat Vectors and Mitigation Options .....</b>	<b>56</b>
3.7.1.	Sensor Spoofing.....	56
3.7.2.	Data Manipulation or Replacement .....	57
3.7.3.	False Identity Claim at Enrollment .....	57
3.7.4.	Imposter Attempts.....	57
<b>3.8.</b>	<b>Biometric Standards.....</b>	<b>57</b>
3.8.1.	Technical Interfaces.....	59
3.8.2.	Data Formats.....	59
3.8.3.	Implementations.....	60
3.8.3.1.	Application Profiles .....	60
3.8.3.2.	Societal Considerations .....	61
3.8.3.3.	Best Practices and Guidance.....	61
3.8.4.	Testing and Reporting.....	61
<b>3.9.</b>	<b>Future Biometric Trends .....</b>	<b>62</b>
<b>3.10.</b>	<b>Biometrics Checklist.....</b>	<b>66</b>
<b>4.</b>	<b>PHYSICAL ACCESS CONTROL SYSTEM (PACS) .....</b>	<b>65</b>
<b>4.1.</b>	<b>Overview.....</b>	<b>65</b>
<b>4.2.</b>	<b>PACS Main Components .....</b>	<b>66</b>
4.2.1.	Emerging PACS Technologies Cards & Readers .....	68
4.2.2.	Near Field Communication (NFC) .....	68
4.2.3.	Cloud Computing in Physical Security.....	68
4.2.4.	Card Types .....	69
4.2.5.	Personal Identification Number (PIN) Utilization .....	70

4.2.6.	Card technologies .....	71
4.2.6.1.	Credential Form Factors .....	72
4.2.7.	Card/Credential Reader Considerations.....	72
4.2.7.1.	Ergonomics Considerations .....	73
4.2.7.2.	Wireless Connectivity Options .....	73
4.2.7.3.	Remote Readers .....	73
4.2.7.4.	Common or Co-Located Vehicle Control Considerations .....	74
4.2.7.5.	Mobile Reader Considerations.....	74
4.2.7.6.	Installation Considerations .....	74
4.2.7.7.	Insertion versus Swipe Readers .....	74
4.2.7.8.	Contactless and Proximity Card Readers.....	74
4.2.7.9.	Smart Card Reader and Data Formats.....	75
4.2.7.10.	Internal Exit Reader Use (case example).....	75
4.2.8.	Portal Door Hardware .....	75
4.2.9.	Field Controllers .....	75
4.2.9.1.	Inter-Device Communication.....	76
4.2.9.2.	Spread Spectrum Communication .....	76
4.2.9.3.	Field Controller Functional Features Summary.....	77
4.2.9.4.	UL Requirements .....	77
4.2.9.5.	Mutual Authentication for PACS.....	78
4.2.10.	PACS Server & Application Software: Main Functions Overview.....	78
4.2.10.1.	PACS Software .....	78
4.2.10.2.	PACS Server Hardware .....	80
4.2.10.3.	PACS Client Workstations .....	81
4.2.11.	Special PACS Use Cases .....	81
4.2.11.1.	Two Person Control.....	81
4.2.11.2.	Elevator Control.....	81
<b>4.3.</b>	<b>Regulatory Requirements and Industry Standards .....</b>	<b>82</b>
4.3.1.	Standards, Regulations and Guidelines Applicable to Airport Access Control Systems..	83
4.3.1.1.	Federal Information Processing Standard (FIPS) 201 .....	83
4.3.1.2.	Personal Identity Verification Interoperability for Non-Federal Issuers .....	83
4.3.1.3.	Underwriter Laboratories (UL) 294.....	83
4.3.1.4.	Underwriter Laboratories (UL) 1076.....	84
4.3.1.5.	National Fire Protection Association (NFPA) .....	84
4.3.1.6.	National Electric Code (NEC) .....	84

4.3.1.7.	Recommended Security Guidelines for Airport Planning, Design and Construction, TSA 2011 and FAA/NSSA 2017 .....	84
4.3.1.8.	ISO/IEC 24727 – Identification Cards – Integrated Circuit Cards Programming Interfaces [Parts 1-6] .....	85
4.3.1.9.	Additional Requirements Imposed on Airport Security Systems .....	85
4.3.1.10.	Approved Products List .....	85
4.3.2.	Environmental Impact to Airport PACS.....	85
<b>4.4.</b>	<b>System Design Issues Overview (Reference ConOps) .....</b>	<b>85</b>
4.4.1.	Throughput at Different Boundary Areas Entry and Exit.....	85
4.4.2.	System Design Considerations - Threats .....	86
4.4.3.	Hardware.....	86
4.4.4.	Software .....	86
4.4.5.	Electrical .....	87
4.4.6.	Environmental.....	87
4.4.7.	Maintenance.....	87
<b>4.5.</b>	<b>Portal Operation.....</b>	<b>87</b>
4.5.1.	Portal position switch.....	87
4.5.2.	Interior Doors.....	88
4.5.3.	Exterior Doors.....	88
4.5.4.	Fire-Rated Doors.....	89
4.5.5.	Automated Exit Lane Breach Control.....	89
4.5.5.1.	Current Situation.....	89
4.5.5.2.	ELBC Goal .....	90
4.5.5.3.	ELBC Examples .....	90
4.5.5.4.	Capability.....	91
4.5.5.5.	Technologies.....	91
4.5.5.5.1.	Microwave (Motion Detection) .....	91
4.5.5.5.2.	Infrared (Presence Detection) .....	91
4.5.5.5.3.	Video (Visible Light).....	91
4.5.5.6.	Intruder Detection .....	92
4.5.5.7.	Object Detection .....	92
4.5.5.8.	Interfaces for Authorized Access.....	92
4.5.6.	Rotating Portals.....	93
4.5.7.	Mantraps .....	93
4.5.8.	Rollup Doors.....	93

4.5.9.	Vehicle Barriers .....	93
4.5.10.	Key and Lock Technologies .....	94
4.5.11.	Other .....	95
4.5.12.	Auditing and Reporting.....	95
4.5.13.	Server Configuration.....	95
4.5.14.	Power Considerations .....	96
<b>4.6.</b>	<b>Authentication Mechanisms; Multiple Authentication and Security Factors.....</b>	<b>97</b>
4.6.1.	PIN-to-PACS as Single Factor Knowledge .....	98
4.6.2.	PIN-to-Card Operation .....	99
4.6.3.	Card with PIN-to-PACS Operation .....	99
4.6.4.	Authentication IT Infrastructure with PKI.....	101
4.6.5.	PACS System Operator Authentication.....	101
4.6.6.	Data Protection: Data at rest .....	102
4.6.7.	Data Protection: Data in Transit .....	102
<b>4.7.</b>	<b>PACS Technology Trends.....</b>	<b>102</b>
4.7.1.	Multifactor Authentication, stand-alone, self-contained reader.....	102
4.7.2.	Card – Reader Mutual Authentication .....	104
4.7.3.	Virtualization .....	104
4.7.3.1.	Mobile Devices as PACS Credentials.....	105
4.7.3.1.1.	What forms of credential are required on mobile devices for PACS?.....	105
4.7.3.1.2.	What technologies are required of mobile devices to host and use a PACS credential? .....	106
4.7.3.1.3.	How do credentials get on the mobile devices and how are they managed? .....	107
4.7.3.1.4.	Mobile Devices as PACS Credentials Summary .....	108
<b>4.8.</b>	<b>Interfaces with Other Systems .....</b>	<b>108</b>
4.8.1.	Access Alarms .....	108
4.8.2.	Intrusion Alarms.....	108
4.8.3.	Portal Operation.....	109
4.8.3.1.	Portal Forced Open .....	109
4.8.3.2.	Portal Open Too Long .....	109
4.8.3.3.	Portal Tamper .....	110
4.8.3.4.	PACS Portal Breaches & Intrusion Detection .....	110
4.8.3.5.	Integration with Video {Video Assessment, Analytics, Storage and Retrieval of Event Video Clips} .....	111
4.8.3.5.1.	Video Alarms.....	111
4.8.3.5.2.	Video Analytic Examples .....	112

<b>4.9.</b>	<b>Pilot Access.....</b>	<b>113</b>
<b>4.10.</b>	<b>Physical Access Control System (PACS) Checklist.....</b>	<b>113</b>
<b>5.</b>	<b>PERIMETER INTRUSION DETECTION .....</b>	<b>119</b>
<b>5.1.</b>	<b>Perimeter Intrusion Detection System Overview .....</b>	<b>119</b>
5.1.1.	Mission.....	119
5.1.2.	Risk and Needs Assessment.....	120
<b>5.2.</b>	<b>Regulatory Requirements .....</b>	<b>120</b>
<b>5.3.</b>	<b>Threats/Vulnerabilities .....</b>	<b>121</b>
<b>5.4.</b>	<b>Current Practices.....</b>	<b>121</b>
5.4.1.	Fencing.....	122
5.4.2.	Sensing Technology.....	122
5.4.3.	Patrol.....	123
5.4.4.	Perimeter Maintenance .....	123
5.4.5.	Best Practices.....	123
5.4.6.	Perimeter Systems Product Testing .....	124
<b>5.5.</b>	<b>Requirements .....</b>	<b>124</b>
5.5.1.	Requirements Overview .....	124
5.5.2.	Requirements Traceability.....	124
5.5.3.	Typical PIDS Requirements.....	124
<b>5.6.</b>	<b>System Design Considerations.....</b>	<b>126</b>
5.6.1.	Design Process.....	126
5.6.2.	System Performance .....	126
5.6.2.1.	Performance Measures.....	126
5.6.2.2.	Layering of Sensing Technologies and Solutions.....	127
5.6.2.3.	Modeling & Simulation (M&S).....	128
5.6.3.	Design Factors and Constraints .....	129
5.6.3.1.	Operational.....	129
5.6.3.2.	Environmental.....	129
5.6.3.3.	Technological.....	129
5.6.3.4.	Infrastructure Driven.....	129
5.6.4.	Tolerance for Change.....	130
5.6.4.1.	Maintainability and Change Management .....	130
5.6.4.2.	Adaptability .....	130
5.6.4.3.	Migration Plan .....	130

5.6.4.4.	Feedback Capture .....	131
<b>5.7.</b>	<b>Industry Standards.....</b>	<b>131</b>
<b>5.8.</b>	<b>Current Technology .....</b>	<b>138</b>
5.8.1.	Introduction.....	138
5.8.1.1.	Pulse Infrared (Exterior) .....	143
5.8.1.2.	Coaxial Cable Technology.....	144
5.8.1.3.	Fiber-Optic Cable .....	144
5.8.1.4.	Underwater Fiber-optic Netting.....	145
5.8.1.5.	Buried Pressure Line Sensor.....	145
5.8.1.6.	Ported Coax Buried Cable .....	146
5.8.1.7.	Taut Wire .....	147
5.8.1.8.	Bi-static Microwave.....	148
5.8.1.9.	Mono-static Microwave .....	149
5.8.1.10.	Electric Field or Capacitance .....	150
5.8.1.11.	Video Motion Detection (VMD) .....	151
5.8.1.12.	Thermal (LWIR) Video Analytics w/GPS Location.....	152
5.8.2.	Assess / Identify / Classify.....	153
5.8.3.	Track / Locate .....	153
5.8.3.1.	Video-Based Tracking (VBT).....	153
5.8.3.2.	Radar Systems .....	153
5.8.3.3.	LADAR Systems.....	154
5.8.3.4.	Geo-spatial Systems.....	155
5.8.4.	Other Technologies.....	156
<b>5.9.</b>	<b>Technology Trends .....</b>	<b>156</b>
5.9.1.	Wireless Technologies .....	156
5.9.2.	Physical Security Information Management Systems (PSIM) .....	156
<b>5.10.</b>	<b>PIDS Integration.....</b>	<b>157</b>
<b>5.11.</b>	<b>Staffing, Training, and Sustainment (Maintenance).....</b>	<b>158</b>
5.11.1.	Staffing Considerations.....	158
5.11.2.	Perimeter Security Training Considerations .....	158
5.11.3.	Sustainment Considerations.....	159
<b>5.12.</b>	<b>References to Previous PIDs Sections.....</b>	<b>159</b>
<b>5.13.</b>	<b>Perimeter Intrusion Detection Checklist.....</b>	<b>159</b>

<b>6.</b>	<b>VIDEO SURVEILLANCE SYSTEMS.....</b>	<b>161</b>
<b>6.1.</b>	<b>System Overview .....</b>	<b>161</b>
<b>6.2.</b>	<b>Imaging Sensor Type.....</b>	<b>162</b>
6.2.1.	Selecting Cameras and Lenses .....	162
6.2.2.	Solid State Video Detectors.....	163
6.2.3.	Thermal Imaging Sensors.....	163
<b>6.3.</b>	<b>Applications .....</b>	<b>164</b>
6.3.1.	Outer Perimeter.....	164
6.3.2.	Landside Terminal Roadways .....	165
6.3.3.	Vehicle Access Gates.....	166
6.3.4.	Portals to Secured Area.....	166
6.3.5.	Security Checkpoints .....	167
<b>6.4.</b>	<b>System Design .....</b>	<b>167</b>
6.4.1.	Imager Operational Performance.....	168
6.4.1.1.	Performance Metrics.....	168
6.4.1.2.	Pixel Density Metrics.....	170
6.4.2.	General Architectures .....	173
6.4.3.	Open Standards .....	175
6.4.4.	Standards Groups.....	175
6.4.5.	US and International Video Standards.....	175
6.4.6.	Security Surveillance Camera Formats.....	177
6.4.7.	Camera Coverage (Field-of-View) .....	177
6.4.7.1.	Megapixel and HD Cameras.....	179
6.4.7.2.	Wide Angle and Multi-Imager Cameras.....	179
6.4.8.	Encoding .....	180
6.4.8.1.	H.264 and H.265.....	180
6.4.8.2.	Additional Encoding Considerations.....	181
6.4.9.	Transmission.....	181
6.4.10.	Viewing.....	181
6.4.11.	Recording and Storage.....	183
6.4.11.1.	Storage Solutions .....	184
6.4.11.2.	Off-Site Remotely Accessible Storage .....	187
6.4.12.	Video Servers.....	188
6.4.13.	Video Management Systems (VMS).....	189

6.4.14.	Video Analytics .....	190
6.4.14.1.	Artificial Intelligence (AI) .....	192
6.4.15.	System and Subsystem Integration .....	192
6.4.16.	Physical Security Information Management (PSIM) Systems .....	193
6.4.17.	Enhancing Legacy Systems with Software .....	193
6.4.18.	Displaying Information in Command Centers .....	194
<b>6.5.</b>	<b>Lighting .....</b>	<b>195</b>
<b>6.6.</b>	<b>System Testing .....</b>	<b>197</b>
<b>6.7.</b>	<b>Regulations.....</b>	<b>197</b>
<b>6.8.</b>	<b>Technology Trends .....</b>	<b>197</b>
<b>6.9.</b>	<b>Video Surveillance Checklist .....</b>	<b>198</b>
<b>7.</b>	<b>SECURITY OPERATIONS CENTER (SOC).....</b>	<b>201</b>
<b>7.1.</b>	<b>Typical Security Operations Center .....</b>	<b>204</b>
7.1.1.	Facilities: Standard SOC Design / Build / Operation Considerations .....	204
7.1.2.	Facilities: SOC Supporting PACS Communications Infrastructure .....	205
<b>7.2.</b>	<b>Security Operations Center (SOC) Requirements .....</b>	<b>205</b>
7.2.1.	Displaying Information in the SOC .....	205
<b>7.3.</b>	<b>SOC and Situational Awareness .....</b>	<b>206</b>
7.3.1.	Continuing Domain Awareness in the SOC.....	207
<b>7.4.</b>	<b>SOC Checklist.....</b>	<b>208</b>
<b>8.</b>	<b>INTEGRATION .....</b>	<b>209</b>
<b>8.1.</b>	<b>Overview.....</b>	<b>209</b>
8.1.1.	A Value Proposition.....	210
8.1.2.	Integration Process.....	212
<b>8.2.</b>	<b>Integrated System Design Considerations and Criteria.....</b>	<b>214</b>
8.2.1.	Integration Architectures .....	215
8.2.2.	Methodologies and Guides .....	216
8.2.3.	Standards.....	218
<b>8.3.</b>	<b>Choosing a Platform.....</b>	<b>219</b>
8.3.1.	VMS-based Platforms.....	220
8.3.2.	Physical Security Information Management (PSIM) Systems .....	220
<b>8.4.</b>	<b>System Component Interoperability.....</b>	<b>221</b>
8.4.1.	System Interfaces .....	222

<b>8.5.</b>	<b>Cost Impacts .....</b>	<b>223</b>
<b>8.6.</b>	<b>Configuration Management/Migration Issues .....</b>	<b>223</b>
<b>8.7.</b>	<b>Additional Users .....</b>	<b>223</b>
8.7.1.	Additional Remote Sites .....	224
<b>8.8.</b>	<b>Integration Trends.....</b>	<b>224</b>
<b>8.9.</b>	<b>Integration Checklist.....</b>	<b>225</b>
<b>9.</b>	<b>COMMUNICATIONS INFRASTRUCTURE.....</b>	<b>227</b>
<b>9.1.</b>	<b>Introduction – Overview .....</b>	<b>227</b>
<b>9.2.</b>	<b>System Requirements Summary .....</b>	<b>228</b>
9.2.1.	Wired Communication Systems .....	228
9.2.1.1.	Telephone Systems .....	228
9.2.1.1.1.	Carrier Based Systems and PBXs .....	228
9.2.1.1.2.	Voice-over-Internet Protocol (VoIP) .....	229
9.2.2.	Wireless Communications Systems.....	229
9.2.2.1.	Cellular Voice and Data.....	229
9.2.2.2.	Trunked Radio Systems and Interoperability.....	230
9.2.2.2.1.	Project 25 (P25) .....	230
9.2.2.3.	DHS Multiband Radios.....	231
9.2.2.4.	VHF and UHF Radios.....	232
9.2.2.5.	DHS SAFECOM Program.....	232
9.2.3.	Commercial Services .....	233
9.2.4.	Wireless IT Networks, also known as Wireless LANs (WLANs).....	233
<b>9.3.</b>	<b>Regulatory Requirements and Standards .....</b>	<b>233</b>
9.3.1.	FCC Role .....	234
9.3.2.	Spectrum Considerations .....	234
<b>9.4.</b>	<b>Threats.....</b>	<b>235</b>
9.4.1.	Public Key Infrastructures (PKIs).....	236
<b>9.5.</b>	<b>Current Practices.....</b>	<b>237</b>
<b>9.6.</b>	<b>Design Objectives.....</b>	<b>238</b>
9.6.1.	Communications Infrastructure .....	238
9.6.2.	Network Standards.....	239
9.6.3.	Network Infrastructure Relationships .....	240
9.6.4.	Communications Functionality .....	240

<b>9.7.</b>	<b>System Design Considerations.....</b>	<b>241</b>
9.7.1.	Performance .....	242
9.7.2.	LAN Protocols .....	243
9.7.3.	OSI Model.....	244
9.7.4.	Topologies .....	244
9.7.5.	VLANs.....	246
9.7.6.	Bandwidth Management .....	246
9.7.7.	Quality of Service (QoS) Issues.....	247
9.7.8.	IP Voice .....	247
9.7.9.	Multicasting .....	248
9.7.10.	Virtual Private Network (VPN) .....	249
<b>9.8.</b>	<b>Network Backbone and Infrastructure .....</b>	<b>249</b>
<b>9.9.</b>	<b>Device Wiring .....</b>	<b>250</b>
9.9.1.	Cabling Management.....	250
9.9.2.	Cable Plant Migration Strategy.....	251
9.9.3.	Wire and Cable Installation .....	251
9.9.4.	Fiber Optic Backbone Cabling.....	252
9.9.4.1.	Fiber Optic Cables and Standards.....	252
9.9.5.	Structured Cabling .....	253
9.9.5.1.	Structured Cabling Types and Standards.....	253
9.9.5.2.	Power-over-Ethernet (PoE).....	255
9.9.5.3.	Color Codes for RJ-45 Ethernet Plug and Jack.....	256
9.9.5.4.	Performance Verification and Testing.....	256
9.9.6.	End Point Connections.....	257
9.9.7.	Complying with Standards.....	258
9.9.8.	Labeling .....	259
9.9.9.	Telecommunication Rooms (TRs).....	260
<b>9.10.</b>	<b>Wireless Networks and Devices.....</b>	<b>261</b>
9.10.1.	Wireless Communications .....	261
9.10.2.	Wireless LANs (WLAN).....	261
9.10.3.	WiFi Wireless LANs .....	263
9.10.4.	WiMAX .....	264
9.10.5.	Long Range WiFi Communications .....	265
9.10.6.	Radio Frequency Identification (RFID).....	265
9.10.7.	Near-Field Communications (NFC) .....	267

9.10.8.	Radio over IP (RoIP) .....	267
<b>9.11.</b>	<b>Privacy and Data Security Considerations.....</b>	<b>268</b>
9.11.1.	Network Security Standards and Guidelines .....	268
9.11.2.	Transmission and Data Security .....	268
9.11.3.	Network Security .....	269
9.11.4.	Cybersecurity .....	269
<b>9.12.</b>	<b>Trends.....</b>	<b>273</b>
<b>10.</b>	<b>GENERAL ACQUISITION RELATED CONSIDERATIONS .....</b>	<b>275</b>
<b>10.1.</b>	<b>Introduction .....</b>	<b>275</b>
<b>10.2.</b>	<b>Regulatory Requirements .....</b>	<b>275</b>
10.2.1.	Federal, State, and Local Regulatory Requirements.....	275
10.2.1.1.	49 Code of Federal Regulation Part 1542, Airport Security.....	275
10.2.1.2.	Federal Security Guidelines.....	276
10.2.1.3.	Disclosure of Security Sensitive Information (SSI).....	276
<b>10.3.</b>	<b>System Acquisition Phase .....</b>	<b>277</b>
10.3.1.	System Design .....	277
10.3.2.	System Design Objectives .....	277
10.3.2.1.	Standards-Based Open Architecture .....	277
10.3.2.2.	Interoperability.....	278
10.3.2.3.	Scalability .....	278
10.3.2.4.	Reliability, Maintainability, and Availability .....	278
10.3.3.	Legacy System Integration .....	278
10.3.4.	System Specification and Selection .....	279
<b>10.4.</b>	<b>System Installation Phase .....</b>	<b>282</b>
<b>10.5.</b>	<b>Implementation Phasing Considerations.....</b>	<b>283</b>
<b>10.6.</b>	<b>System Documentation.....</b>	<b>283</b>
10.6.1.	As-Built Drawings and Bill of Materials .....	283
10.6.2.	Operational Procedures Format and Content.....	283
<b>10.7.</b>	<b>Training Manuals and Courses .....</b>	<b>284</b>
10.7.1.	ISSA Operator Training.....	284
10.7.2.	Systems Administrator Training .....	284
10.7.3.	Maintenance Training.....	285
10.7.4.	Biometrics – Special User Training Considerations.....	285
<b>10.8.</b>	<b>System Test, Verification and Validation.....</b>	<b>285</b>

10.8.1.	System Test.....	286
10.8.1.1.	System Test Plan Development .....	286
10.8.1.1.1.	Testing of Revisions or Upgrades.....	287
10.8.1.2.	System Test Procedure Development (STProc).....	287
10.8.1.3.	System Qualification and Acceptance Testing (SQT) .....	287
10.8.1.4.	Site Installation Testing (SIT).....	288
10.8.1.5.	Operational Transition Plan .....	288
10.8.1.6.	Operational Testing.....	288
10.8.2.	Special Biometric Subsystem Testing and Certification.....	289
<b>10.9.</b>	<b>Warranty Requirements .....</b>	<b>289</b>
<b>10.10.</b>	<b>System Logistics Support.....</b>	<b>289</b>
10.10.1.	Maintenance Considerations .....	290
<b>11.</b>	<b>MEMBERSHIP .....</b>	<b>291</b>

**APPENDIX A – STANDARDS.....A-1**

<b>A.1</b>	<b>FEDERAL, STATE, AND LOCAL.....</b>	<b>A-2</b>
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 Agencies .....	A-2
<b>A.2</b>	<b>Industry and International Standards.....</b>	<b>A-3</b>
A.2.1	Construction Specifications Institute (CSI), MasterSpec (2004) .....	A-3
A.2.2	Institute of Electrical and Electronics Engineers (IEEE) .....	A-3
A.2.3	International Civil Aviation Organization (ICAO) .....	A-3
A.2.4	International Organization for Standardization (ISO) .....	A-3
A.2.5	National Electrical Manufacturers Association (NEMA) .....	A-4
A.2.6	National Fire Protection Association (NFPA).....	A-4
A.2.7	Underwriters' laboratories (UL) .....	A-4
<b>A.3</b>	<b>Other References.....</b>	<b>A-4</b>

<b>APPENDIX B – GLOSSARY .....</b>	<b>B-1</b>
<b>APPENDIX C – REFERENCES .....</b>	<b>C-1</b>
<b>APPENDIX D – IDENTITY MANAGEMENT SYSTEMS (IDMS) .....</b>	<b>D-1</b>
<b>D.1 Overview.....</b>	<b>D-1</b>
<b>D.2 Components and Functions.....</b>	<b>D-1</b>
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.2.3.1 Intelligent Cameras.....	D-2
D.2.3.2 Biometric Capture Devices.....	D-2
D.2.3.3 Document scanners.....	D-2
D.2.3.4 Interactive Touchscreen Devices.....	D-2
D.2.3.5 Electronic Signature Capture Devices.....	D-2
D.2.3.6 Badge Printers.....	D-3
D.2.3.7 Other Printing Systems.....	D-3
<b>D.3 Optional Credentialing Capabilities.....</b>	<b>D-3</b>
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-4
D.3.6 Scheduling Management.....	D-4
D.3.7 Data Management/Record Keeping.....	D-4

**TABLE OF FIGURES**

Figure 1-1: Notional Airport Layout.....	3
Figure 1-2: Notional Perimeter Security and Zones .....	6
Figure 1-3: Notional Security Operations Center (SOC).....	7
Figure 2-1: Overview of an Airport Credentialing Process. ....	22
Figure 3-1 Generic Biometric Processes.....	46
Figure 4-1: Sample PACS configuration .....	67
Figure 4-2: Sample PACS and IDMS Components .....	67
Figure 4-3: Cards and Card Data Current Industry Trends .....	71
Figure 4-4: Typical Master Key Schema .....	94
Figure 4-5: Reader to Controller Data Flow .....	98

Figure 4-6: Generic PKI-enabled PACS Configuration.....	101
Figure 5-1: Typical PIDS Progression .....	120
Figure 6-1: Spectral Regions Used by Visible and Infrared Imaging Sensors.....	161
Figure 6-2: Portal Surveillance Concept Diagram .....	167
Figure 6-3: Line-pair Illustration (1 lp = 2 TV pixels).....	169
Figure 6-4: Determining Pixel per Foot (PPF) Values.....	171
Figure 6-5: Camera Angular Coverage and Typical Performance Values.....	173
Figure 7-1: Typical SOC Information Flow Diagram.....	203
Figure 7-2: Examples of SOC Configurations – Small / Medium / Large.....	206
Figure 8-1: Developing an Integrated Airport Security System.....	209
Figure 8-2: Security Integration Functions and Processes .....	212
Figure 8-3: Integrated Security System for Airports (ISSA) Conceptual Design .....	214
Figure 8-4: Peer to Peer Architecture Connectivity .....	215
Figure 8-5: Hierarchal Architecture Connectivity.....	215
Figure 8-6: Systems Engineering Process .....	216
Figure 9-1: Airport Communications Diagram.....	227
Figure 9-2: Frequency Band Allocations .....	231
Figure 9-3: Spectrum Band and Frequency Assignment .....	235
Figure 9-4: Communication Relationship.....	240
Figure 9-5: Communication Services.....	241
Figure 9-6: OSI Stack .....	244
Figure 9-7: Network Topologies.....	244
Figure 9-8: Network Elements Configured for Redundancy .....	245
Figure 9-9: T568A and T568B Pin / Pair Assignments .....	256
Figure 9-10: Typical RFID Components .....	266
Figure D-1: A sample IDMS and Devices Structure.....	D-1

## TABLE OF TABLES

Table 1-1: Airport Security Areas of Concern, Threats and Countermeasures.....	11
Table 4-1: PACS Standard Components.....	66
Table 4-2: Contactless Smart card vs. Proximity Card Technologies.....	69
Table 4-3: PACS & Level of Assurance.....	70
Table 5-1: Example of Key Performance Parameters.....	127
Table 5-2: System Type – Sensor Technology Pd Comparison .....	128
Table 5-3: Typical PIDS-related Standards .....	135
Table 5-4: Perimeter Sensors .....	148
Table 6-1: Examples of Line-Pair Applications.....	170
Table 6-2: Common Camera Types and Their Pixel Counts .....	177
Table 6-3: Angular and Linear Field Coverage for Camera-Lens Combinations.....	180
Table 6-4: Horizontal and Vertical Resolution of US and European Video Standards .....	182
Table 6-5: Digital TV Display Formats for 4:3 Aspect Ratio.....	182
Table 6-6: Digital TV Display Formats for 4:3 16:9 Aspect Ratio.....	183
Table 6-7: Redundant Array of Independent Disks (RAID) Levels .....	186
Table 6-8: Typical Illumination Standards .....	195
Table 9-1: Gigabit Ethernet Fiber Optic Cabling Types and Distances.....	252
Table 9-2a: TIA Cable Classifications and Standards .....	254
Table 9-2b: ISO Cable Classifications and Standards .....	255
Table 9-3: IEEE WLAN Standards.....	261
Table 9-4: Characteristics of IEEE WLAN Standards.....	263
Table 9-5: Evolution of the 802.11 Standards.....	264

## 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, 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.

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 the PACS design provisions remained largely unchanged, details of their implementation and operation has been modified regularly since, primarily by improvements in technology as well as TSA-issued Security Directives and ASP amendments that modify performance requirements.