PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0030 August 2021

Guidance for Access Control System Transitions

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Andrew Goldsmith, Principal Investigator
Anne Marie Pellerin
Michal Rottman
LAM LHA USA, LLC
Alexandria, Virginia

Ann Barry
David McGhee
Carolyn Hughes
Ross & Baruzzini
St. Louis, Missouri

© 2021 National Safe Skies Alliance, Inc. All rights reserved.

COPYRIGHT INFORMATION

Authors herein are responsible for the authenticity of their materials and for obtaining written permissions from publishers or persons who own the copyright to any previously published or copyrighted material used herein.

National Safe Skies Alliance, Inc. (Safe Skies) grants permission to reproduce material in this publication for classroom and not-for-profit purposes. Permission is given with the understanding that none of the material will be used to imply Safe Skies or Federal Aviation Administration (FAA) endorsement of a particular product, method, or practice. It is expected that those reproducing the material in this document for educational and not-for-profit uses will give appropriate acknowledgment of the source of any reprinted or reproduced material. For other uses of the material, request permission from Safe Skies.

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee but can be submitted at any time.

A project panel is formed for each funded Problem Statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request of proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0030 PROJECT PANEL

Martina Benedikovicova *Charlotte Douglas International Airport*
Paul Berumen *Phoenix Sky Harbor Int'l Airport*
Phaedra Fatuesi *Port of Seattle*
Richard King *Sioux Falls Regional Airport*
Cole Lail *National Safe Skies Alliance*
Scott Lawson *Horton Automatics*
Mike Pilgrim *ISC International Security Concepts*
Renè Rieder *Burns Engineering*
Christer Wilkinson *AECOM*

AUTHOR ACKNOWLEDGMENTS

LAM LHA would like to acknowledge the following for their contributions in the development of this guidance document:

- National Safe Skies Alliance's PARAS, which provided funding. Particular thanks are given to the program manager, Jessica Grizzle.
- The PARAS 0030 Project Panel members, who also provided significant review and contributions.
- The airports and Access Control System (ACS) subject matter experts who generously provided input for this report through interviews:
    - AECOM
    - Albuquerque International Sunport
    - Baltimore-Washington International Airport
    - Charlotte Douglas International Airport
    - Convergint
    - Dallas-Fort Worth International Airport
    - Denver International Airport
    - Eugene Municipal Airport
    - General Mitchell International Airport (Milwaukee)
    - Kansas City International Airport
    - Phoenix Sky Harbor International Airport
    - Punta Gorda Airport
    - San Antonio International Airport
    - Seattle-Tacoma International Airport
    - Sioux Falls Regional Airport

Richard Duncan, formerly with Atlanta Hartsfield International Airport, also provided valuable input to the document.

Finally, this research would not have been possible without the help of LAM LHA's project partners, Ross & Baruzzini. In particular, appreciation is given to:

- Carolyn Hughes, Project Manager
- David McGhee, Subject Matter Expert – ACS Technology
- Ann Barry, Subject Matter Expert – Aviation Security

CONTENTS

TABLES & FIGURES

EXECUTIVE SUMMARY

This guidance document provides aviation professionals with considerations, pitfalls, and lessons learned during the Access Control System (ACS) selection, procurement, and implementation process. It includes information that applies to airports of various types and sizes that are considering replacing or upgrading their existing ACS, and aims to help reduce risks and costs associated with such an effort.

The guidance is organized using the ACS Transition Process, which establishes a framework for decision-making and activities associated with the transition of the system. The ACS Transition Process consists of discrete, logically connected phases, and serves as a framework for the research findings presented. The document provides users with helpful checklists for each phase of the ACS Transition Process.

The guidance addresses the applicability of regulatory requirements and considerations, including the impact of federal, state, and local laws and regulations on the ACS Transition Process. It also details the evolution of ACS technology and the interrelated topics of data protection of personally identifiable information (PII), biometric technology, and data privacy.

PARAS ACRONYMS

ACRP	Airport Cooperative Research Program
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ACI	Airports Council International
ACS	Access Control System
AES	Advanced Encryption Standard
AHJ	Authority Having Jurisdiction
ASAC	Aviation Security Advisory Committee
ASP	Airport Security Program
ASSIST	Airport Security Systems Integrated Support Testing
BIPA	Biometric Information Protection Act
CAD	Computer-Aided Dispatch
CBP	Customs and Border Protection
CBT	Computer-Based Training
CCPA	California Consumer Privacy Act
CHRC	Criminal History Records Check
DAC	Designated Aviation Channeling
DES	Data Encryption Standard
FIS	Federal Inspection Station
GAO	Government Accountability Office
GLBA	Gramm-Leach-Bliley Act
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
IDMS	Identity Management System
ISSA	Integrated Security System for Airports
LAN	Local Area Network
MAC	Media Access Control
OSDP	Open Supervised Device Protocol
PACS	Physical Access Control System

PII	Personally Identifiable Information
PIN	Personal Identification Number
PoE	Power over Ethernet
PSIM	Physical Security Information Management
REX	Request-to-Exit
RFQ	Request for Qualifications
RTCA	Radio Technical Commission for Aeronautics
SDK	Software Development Kit
SHIELD Act	Stop Hacks and Improve Electronic Data Security Act
SIO	Security Identity Object
SSN	Social Security Number
UL	Underwriters Laboratories
VSE	Virtual Server Environment
VSS	Video Surveillance System

SECTION 1: INTRODUCTION

The need to manage and control the access of individuals and vehicles to secure and non-public areas is a universal and long-standing requirement under TSA regulation 49 CFR § 1542 for US airports. Management and oversight of access control in airport operating environments is a significant undertaking for airport operators, and represents a complex, interconnected set of requirements, systems, and procedures. The continuous and effective operation of these systems is integral to the overall operation of the airport, and represents a key aspect of the security posture of any airport facility.

Commercial airports are subject to a body of federal, state, and local regulations related to airport security and safety. While these regulations do not specify which technologies and systems an airport must use, all TSA-regulated airports must develop an Airport Security Program (ASP), which is approved by TSA and documents measures the airport will take to ensure the control of access to secure areas. The practical effect has been that all US commercial airports operate some type of security portal control within the facility. For a large percentage of commercial airports, this typically entails the use of an Access Control System (ACS).

ACSs often include a complex combination of technology, personnel, and processes that touch many other aspects of the airport's operation. Furthermore, an ACS can represent a major capital and operating investment for airports. Depending on the size of the airport, an ACS can encompass hundreds of doors, portals, barriers, and other access and entry points. An ACS often requires computer servers, cabling, and other infrastructure, and is typically integrated with other airport IT systems. The ACS may be used by hundreds or thousands of airport and airline employees, vendors, contractors, law enforcement and first responders.

As an airport's security, business, and operational needs mature, and as regulations change and technology evolves, airports are eventually confronted with the question of whether their ACS needs to be upgraded or replaced. Once upgrading or replacing the ACS is under consideration, airport managers must address the question of how to transition their ACS so that it meets the airport's requirements in an efficient and cost-effective manner with minimal risks.

The type of ACS and transition chosen will be highly dependent upon the size of the airport and the complexity of the existing systems. Smaller airports may have straightforward implementations and systems with minimal integrations. Larger facilities may have more complex systems and environments with additional integrations. The overall implementation should be scaled to be appropriate to the facility needs and the level of support available for the system.

Implementation and integration of a new or upgraded ACS is a complex, costly, and operationally impactful process for airport operators and security managers. It is important that decision-making for these activities be supported by detailed guidance that allows operators to consider the complex conditions, risks, and best practices associated with access control technology selection, procurement, and implementation.

This guidance document is focused on helping airports effectively navigate the transition of the ACS. Its overall objective is to provide practical information and guidance that will help airports of all sizes address these challenges through research, lessons learned, and best practices, and includes the following:[1]

[1] This document addresses centrally monitored ACSs. The authors recognize that some smaller airports may not use these, but rather use keys or cyberkeys to meet access control requirements. In those cases, the use of this guidance may be limited.

- An overview of the key components of modern ACSs and their evolution, to mitigate the risk of rapid system obsolescence
- A framework for assessing whether an existing airport ACS needs to be upgraded or replaced
- Lessons learned by airports to ensure a successful transition to a new ACS, and ACS transition checklists that reflect these learnings
- Considerations for integrating an ACS with existing airport infrastructure and IT networks
- An overview of the relevant federal, state, and local regulations and laws that may pertain to an airport ACS transition project, with a particular focus on issues related to PII and biometrics

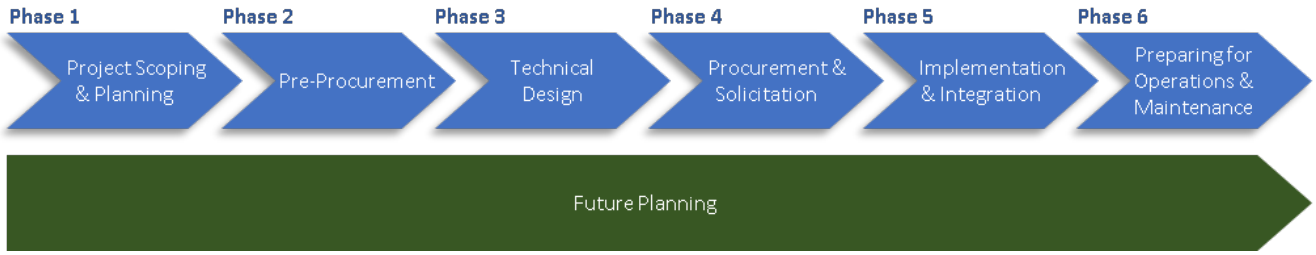
As discussed in greater detail in the following sections, this research indicates that, while each airport has unique ACS requirements, the process of transitioning these systems presents categories of challenges that are common to all airports. These include but are not limited to:

- Organizational – i.e., challenges associated with airport governance, leadership, and the needs of different airport stakeholders and end users that can be involved in different aspects of an ACS transition
- Resource-related – i.e., challenges associated with the time, money, and staff required to transition an ACS
- Technical and operational – i.e., challenges associated with implementing technologies that will effectively support the airport's required security and business operations

1.1 ACS Transition Process Framework

While this guidebook includes a discussion of current and emerging ACS-related technology, its focus is on the individual process steps that make up an ACS transition from beginning to end. This framework is a result of the authors' research. One key finding in the research literature review and subject matter expert interviews was that most ACS transition projects consist of a logically connected set of phases that make up what is referred to here as the "ACS Transition Process." While each airport will vary the sequence of phases they follow and how they name them, airports interviewed generally followed the process shown in Figure 1.

Figure 1. ACS Transition Process



The research identified best practices within each phase of this process for all airports, independent of their unique, airport-specific requirements. Furthermore, the ACS Transition Process phases were used to organize key findings, and the resulting guidance is grouped by ACS Transition Process Phase.

1.2 Research Approach

The research approach was based on two primary efforts: (1) a literature review, and (2) interviews with airport staff and ACS technology subject matter experts.

1.2.1 Literature Review

The research team analyzed approximately 30 documents, including recent PARAS reports, documents from the Radio Technical Commission for Aeronautics (RTCA), academic research on airport security and access control, and a variety of government reports. The literature review provided useful context regarding regulatory, security, and technology drivers that impact an airport ACS. Of particular note, the 2019 edition of RTCA's *DO-230J Standards for Airport Security Access Control Systems* (RTCA DO-230J) provided a framework for understanding the technical and operational components of an airport ACS and other airport security systems that can be integrated with an ACS.[2]

The outputs from the literature review are included in Appendix D.

1.2.2 Interviews

The research team interviewed airport managers involved in ACS transitions, as well as airport ACS technology experts. A total of 20 airport ACS subject matter experts at 13 US airports were interviewed. The team also interviewed three non-airport ACS subject matter experts. All individuals interviewed willingly shared information and relevant ACS materials, including lessons learned and best practices related to ACS transitions.

Interviews were conducted at US airports that had either recently completed or were in the process of completing an ACS upgrade or replacement. A standard interview guide was developed and used to gather insights related to each phase of an ACS transition.

The interviews focused on identifying lessons learned related to an ACS transition that would be applicable to other airports. Specifically, interviewers discussed each phase of the ACS Transition Process, seeking to determine key takeaways from each phase. What follows is a consolidation of the insights gained during these interviews, and the guidance is reflective of the experience of several different airports.

A list of the interviews conducted is attached as Appendix A.

[2] Radio Technical Commission for Aeronautics, Inc. (RTCA), *DO-230J Standards for Airport Security Access Control Systems (DO-230J)*, 2019.

SECTION 2: DEFINING ACS IN US AIRPORTS

2.1 Functional Definition of Airport ACS

A finding from the literature review and interviews is that the term airport *Access Control System* is not precisely defined. Among airport security managers interviewed, there were differences regarding the boundaries of an ACS, precisely what functions and components are included in an ACS, and what functions are integrated with or external to it.

This raised important questions: When we discuss ACS transitions, what is in scope? What specific processes, activities, technologies, and functions are we referring to?

To resolve this issue, the research team relied on the definitional framework provided by the 2019 edition of RTCA DO-230J. This document, developed by a cross-section of aviation security experts, provides useful concepts for establishing the scope of this analysis. Of the documents reviewed in the research, the RTCA document is the most comprehensive in its examination of airport ACS and its definition of ACS components.

Physical Access Control Systems (PACS). According to the RTCA DO-230J, this includes "portals, barriers, card readers, field controllers, and servers that control the entry of persons and identified vehicles and equipment into secured areas."[3] For the purposes of this guidance document, the term "ACS" is treated as synonymous with "PACS" unless otherwise indicated.

Identity Management System (IDMS). According to the RTCA DO-230J, this system controls and manages the issuance and maintenance of access credentials to individuals at an airport.[4] The IDMS is usually integrated with the PACS. The RTCA DO-230J states that the PACS and IDMS are the two main components that address airport access control. For the purposes of this document, an IDMS is a separate system from an ACS. It is an optional system that interfaces to an ACS but is not part of an ACS. It is not a core ACS component, as many airports do not have an IDMS.

Video Management System (VMS). According to the RTCA DO-230J, the VMS, like the IDMS, is a separate system that may interface to an ACS. The VMS is, "the infrastructure and tools for the management of video surveillance systems, including the recording, transmission, viewing, analytics and event management of video … It is often integrated directly to ACSs so that alarms may be exchanged, and video tagged as events occur."[5]

Integrated Security System for Airports (ISSA). Finally, RTCA DO-230J includes the concept of an ISSA. This is a holistic concept that includes an ACS and other systems that together support the security operations of an airport, including alarm monitoring, credentialing, identity management, operations centers, communications infrastructure, biometrics, video management, and intrusion detection. This definition is useful because it places the ACS within the context of a larger set of airport security-related systems that can work alongside and with the ACS.[6]

[3] RTCA, DO-230J, page 8
[4] RTCA, DO-230J, page 8
[5] RTCA, DO-230J, page 189
[6] RTCA, DO-230J, page 8

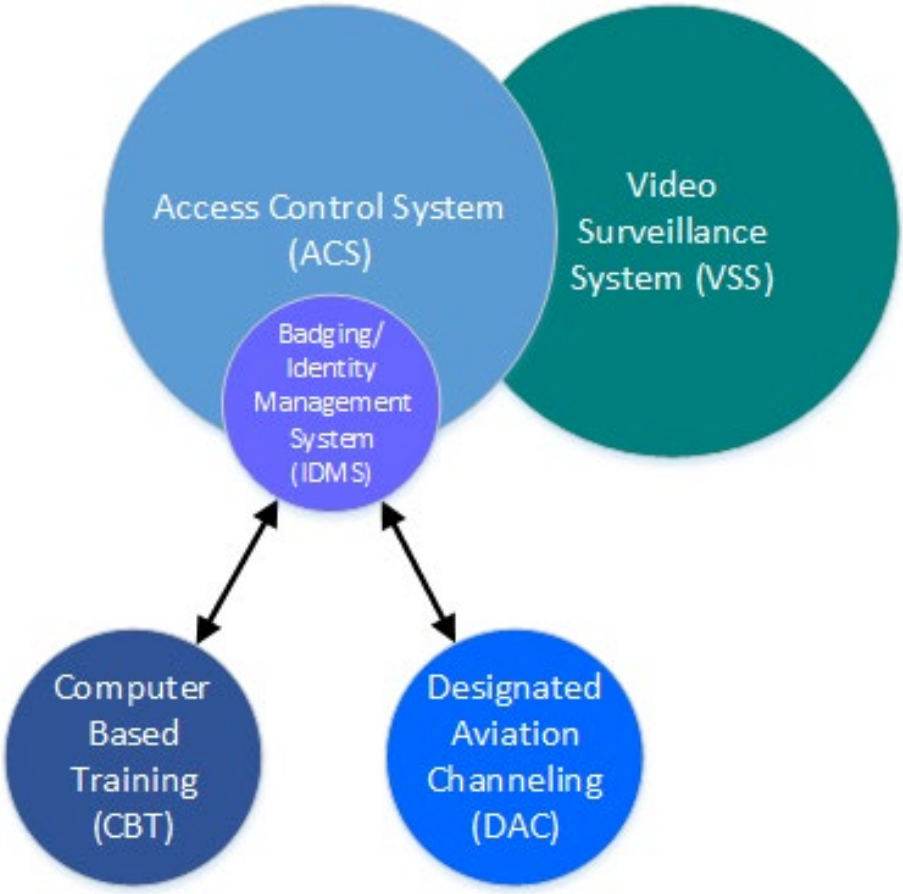
2.2 Typical Airport ACS Configurations

This section provides illustrative and notional representations of an airport ACS. Based on the research, it is recommended that an airport develop a similar diagram to document how its ACS relates to other airport security systems and operations. This section describes a non-exhaustive sample of different ACS architectures, and provides some general considerations related to the potential advantages and limitations associated with each different ACS architecture type.

For the purposes of this discussion, a tightly integrated solution is one in which the component systems' software may be developed by two separate companies, but have been integrated to operate seamlessly together within a single user interface, and this integration is a standard product offered by the manufacturers. An integral solution is where a single manufacturer offers all of the components, and these products are designed to be seamlessly integrated and allow the use of a single user interface.

2.2.1 ACS with Integral/Tightly Integrated Credentialing and VSS

Figure 2. ACS, VSS, IDMS, CBT, and DAC – Tightly Integrated



ACS Architecture Type	Potential Advantages	Potential Limitations
ACS with Integral Credentialing and VSS, and Integrated to CBT and DAC	Integrations between Credentialing, ACS, and VSS are maintained by the system manufacturer(s)	Airport tied to specific manufacturer(s) for multiple systems
	Single user interface for all applications	Limited product offerings during procurement
	Simplified maintenance	May not provide the ability to choose best options for each system due to agreements / offerings

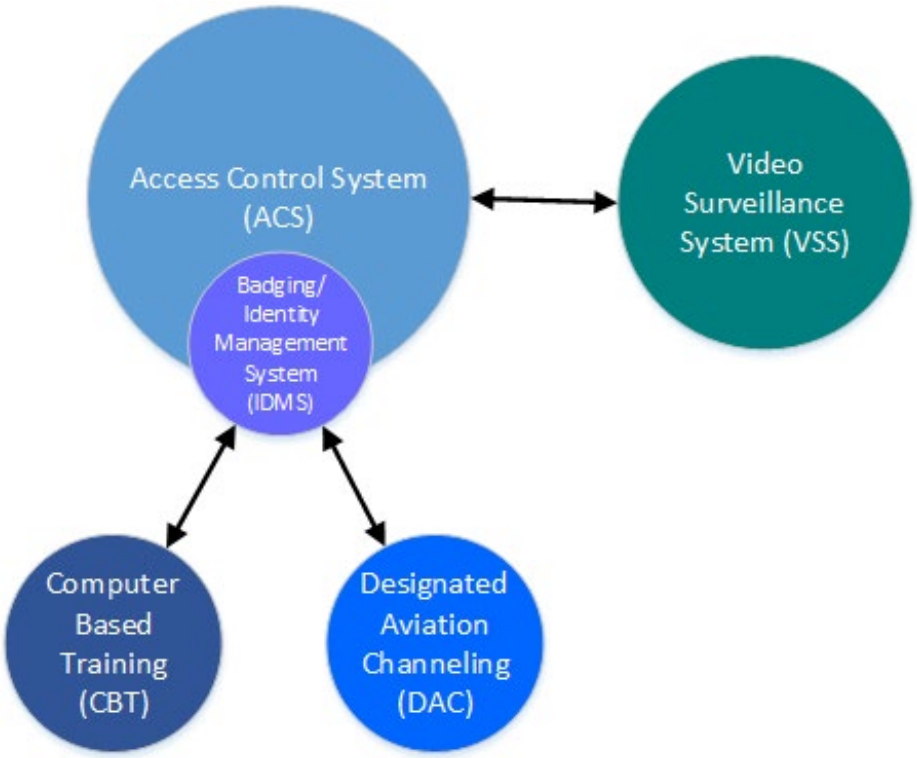
Some vendors in the marketplace have ACS (with integral credentialing) that is tightly integrated with a Video Surveillance System (VSS), or have a single product that has both ACS (with integral credentialing) and VSS. For these types of solutions, illustrated in Figure 2, the manufacturer has a partner that has an exclusive agreement for a highly integrated or integral system that can use a single Graphical User Interface (GUI) for the monitoring, assessment, and response to alarm events for both the VSS and ACS. This type of system is capable of providing call-up and display, and most systems like this can also save data needed to access video related to specific ACS alarm events, allowing for a full review within the single user interface.

While this approach will tie the airport to a specific manufacturer for multiple systems, the overall maintenance will be greatly simplified, as the integrations between the ACS, VSS, and Credentialing are maintained by the manufacturer. In this example, only external systems such as the Computer-Based Training (CBT) and Designated Aviation Channeling (DAC) (if applicable) would need to be integrated, with those integrations requiring maintenance or support. This is also the simplest system from an operational perspective, with the system users all working within a single application.

This approach may not provide all of the features that the airport may desire, but typically will simplify the system operation and maintenance. If an airport wants systems from different vendors for the credentialing/IDMS, ACS, and VSS, this approach may not be suitable, as the offerings will be limited to the specific offerings available from either a single manufacturer or manufacturers that have partnered to offer this type of product.

2.2.2 ACS with Integral Credentialing and Integrated to VSS, CBT, and DAC

Figure 3. ACS with Integral Credentialing and Integrated to VSS, CBT, and DAC



ACS Architecture Type	Potential Advantages	Potential Limitations
ACS with Integral Credentialing and Integrated to VSS, CBT, and DAC	Credentialing/IDMS database is integral to the system and will always be synchronized	Additional integration to be implemented, which may increase the initial cost and ongoing maintenance costs
	Integral credentialing/IDMS are typically less expensive than third-party systems	Integration will typically not be as comprehensive as the previous option
	ACS to VSS integrations are fairly common in the security environment and are typically a simple effort	System operators may need to use multiple interfaces to assess and respond to alarms and events

Most ACS have some form of integral credentialing application, illustrated in Figure 3, although the features and capabilities offered by those integral applications vary widely among manufacturers. If the integral application is acceptable and will meet the needs of the airport, this can save substantial costs, including ongoing maintenance and licensing costs.

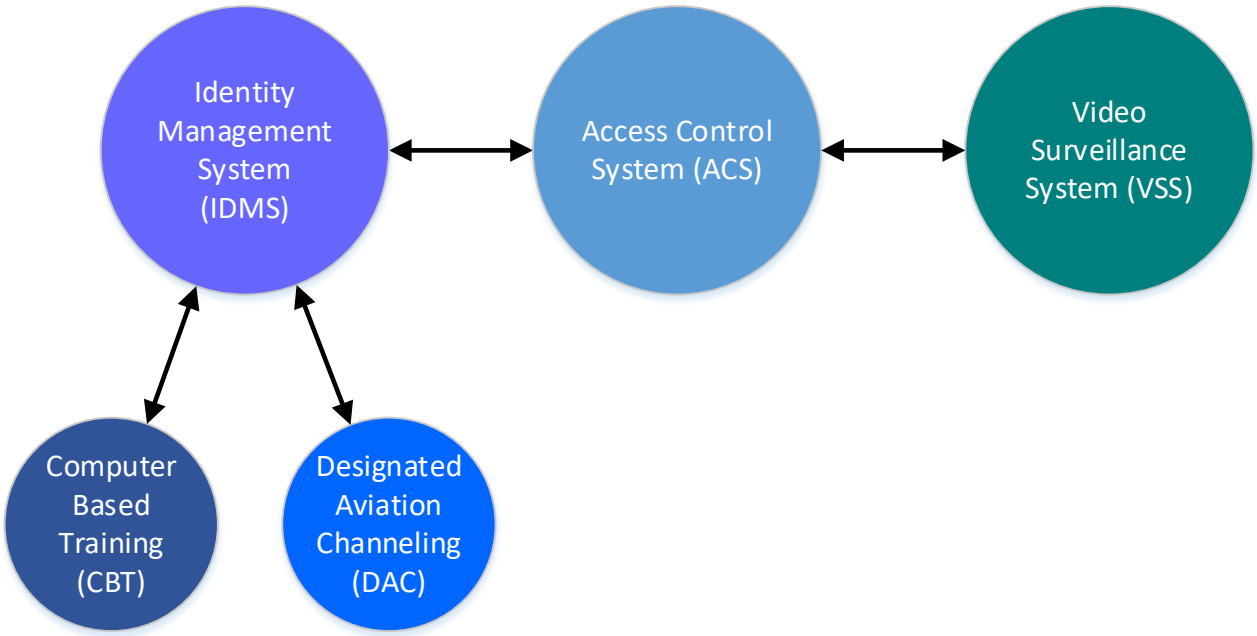
In this configuration, the ACS would address all user data, portal control, access rights, and the recording of data related to transactions and alarm events as defined in the system. However, the call-up of video would be an external link, and the video would most likely be called up within a separate application, either on the same monitor or a separate monitor at the workstation. Depending on the level of integration possible, the ability to index video to an ACS alarm event may or may not be available.

Also, whenever an upgrade to the ACS or VSS is required, the integration will need to be tested to ensure that it is not impacted.

This type of system configuration may be slightly more difficult for system operators, as they will need to be trained on both the ACS and VSS applications, and will have to move between the two applications as needed. The CBT and DAC integration would be similar to the previous configuration.

2.2.3 ACS Integrated to IDMS and VSS

Figure 4. ACS Integrated to IDMS and VSS



ACS Architecture Type	Potential Advantages	Potential Limitations
ACS Integrated to VSS and IDMS, with CBT and DAC integrated to the IDMS	Allows airport to select the best fit for each system with features desired	Additional integrations to be implemented, which will likely raise the initial cost as well as the ongoing maintenance costs
	ACS will not need to offer the IDMS features, allowing selection of ACS based on other factors	Additional auditing may be required to ensure that the IDMS and ACS databases are fully synchronized (exception audits)
	ACS is not impacted by CBT and DAC upgrades	Integration between ACS and VSS will typically not be as comprehensive as the first option
	ACS is dedicated to access control-related tasks only	System operators may need to use multiple interfaces to assess and respond to alarms and events

If the airport requires features that are not available within the integral credentialing applications offered by ACS manufacturers, then a standalone IDMS may be considered. The IDMS would be integrated

with other systems such as the CBT and DAC, as these are specific to the IDMS function. As illustrated in Figure 4, the IDMS would be integrated with the ACS to provide data required for the ACS to operate and report correctly, but the majority of the credential-holder data would be maintained in the IDMS.

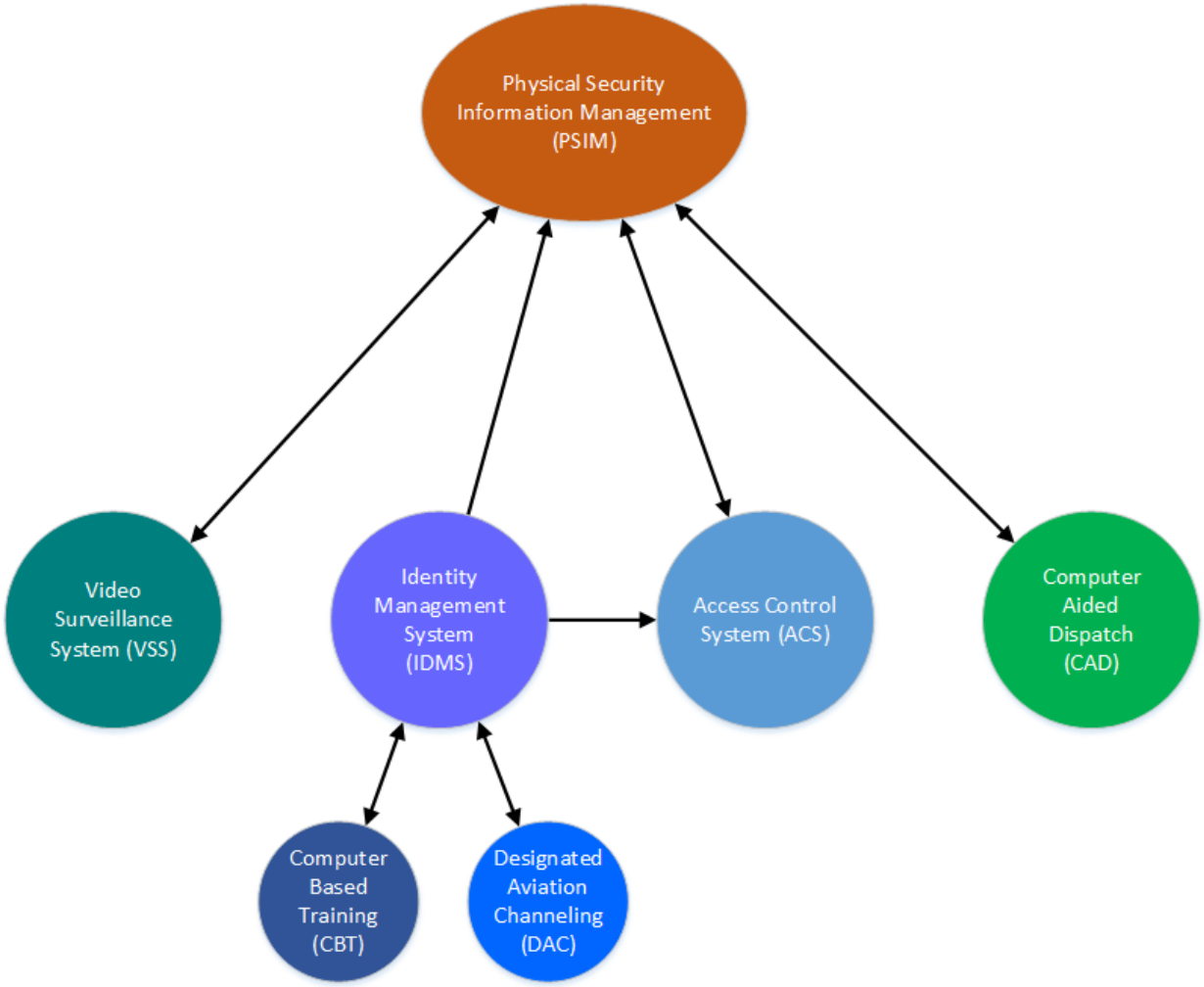
The use of a separate IDMS allows for credentialing personnel to only be trained on the IDMS GUI, as all credentialing functions will occur within that single user interface. Data such as the credential holder name, company, credential number, access rights, and possibly photo would be transferred to the ACS to allow for display upon alarm. The level of integration between the ACS and IDMS can vary. For example, the interface may allow for credential status changes to be made in the ACS, while other systems require those changes be made in the IDMS to prevent data conflicts. Regardless, the data in the two systems will need to be synchronized, and their differences should be documented for correction by creating an exception report.

Similar to the scenario illustrated in Figure 3, the ACS will also be integrated with the VSS for video call-up. In this configuration, the integrations and complexity increase, which can impact the ongoing costs and maintenance. The user experience for the system operators also becomes more complex, as there are more applications that need to be accessed to accomplish system tasks.

While the IDMS offerings in the marketplace provide significant features and capabilities, the costs associated with these systems can be higher. As the number of integrations increase, the maintenance and testing of upgrades to each system can also increase, requiring a higher level of IT governance over the systems. These types of configurations are more common at airports that have greater IT and integrator support capabilities, and have a need for the features offered by a standalone IDMS.

2.2.4 ACS and Other Security Systems Integrated to PSIM

Figure 5. ACS Integrated to PSIM



ACS Architecture Type	Potential Advantages	Potential Limitations
ACS and Other Security Systems integrated to PSIM	ACS is a subsystem that is dedicated to access control, and is only integrated to the PSIM and the IDMS	Overall security environment is much more complex to maintain
	The integration to the PSIM is typically by the PSIM Manufacturer/Integrator, so costs are not on the ACS	PSIM integration and environment will limit ability to upgrade the ACS
	The ACS GUI will not be used for monitoring, so the quality of the ACS GUI is not as important as it would be without a PSIM	Integration is dependent upon the PSIM for most interfaces. If the PSIM is not operational, integrations may not be available.
	Operators will be trained primarily on the PSIM user interface and will generally not use the ACS	Depending upon the PSIM, not all features of the ACS may be available within the PSIM interface, requiring operators to access the ACS for select functions or tasks

Some airports use a PSIM system as the primary user interface between most of the security systems, as illustrated in Figure 5. A PSIM will typically act as a top-of-systems integration platform, controlling the interaction of the various security subsystems. For example, an alarm from the ACS would be transferred to the PSIM, and upon a PSIM operator selecting the alarm for assessment, the PSIM would provide the video associated with the alarm for assessment, allow for data entry relating to the alarm, and support a full resolution of the alarm in the PSIM GUI. Depending upon the integration to the ACS, the details of the alarm may be sent to the ACS for acknowledgement and to allow for reports to be run within the ACS. The PSIM will be able to index video from the VSS related to the alarm, and will be able to pull additional data from the IDMS as needed for additional alarm response. The downside of this type of configuration is that if the PSIM is not operational, none of the integrations managed by the PSIM may be available until the PSIM is restored.

For this type of scenario, the PSIM will be the primary user interface and the operators will only need to be trained on the single GUI. However, system administrators and supervisory personnel will likely need to be trained on the PSIM and each of the various subsystems, as most PSIM applications do not offer all of the features required for reporting and other similar functions. For the system operators that assess and respond to alarm events, the PSIM will provide a very uniform user interface. Likewise, as in other configurations, the use of an IDMS allows for credentialing personnel to only be trained on the IDMS GUI, as all credentialing functions will occur within the IDMS user interface.

While this type of configuration may provide benefits for credentialing personnel and the security system operators, the complexity of these systems and the costs associated with them may be a limiting factor for many airports. Similar to the IDMS, a PSIM can require substantial capital investment to procure and implement, and may have significant ongoing maintenance costs, including the integrations between the disparate systems in addition to the PSIM licensing and maintenance costs. The maintenance and testing of upgrades to each subsystem can become a significant effort, requiring a much higher level of IT governance over the systems. A change to any subsystem could impact the PSIM and cause a system failure, so extensive testing and careful configuration control will be required for each subsystem, with only PSIM manufacturer-approved upgrades being implemented. These types of configurations tend to be more common at airports that have substantial IT and integrator support capabilities, and have a need for the features offered by a standalone IDMS and a PSIM.

In addition to the systems noted above, a CAD is also shown in Figure 5.[7] CAD systems tend to be more common at facilities where the Operations Center is also a Public Safety Answering Point, more commonly referred to as a 9-1-1 center.

The introduction of a CAD, either in the place of a PSIM or in addition to a PSIM, needs to be carefully considered, as a CAD system used for 9-1-1 applications can have other issues such as limitations on integration or privacy regulations. As policies and systems vary between states or regional districts, the individual systems and the policies will need to be researched and considered. This adds another level of complexity, and the use of any of these systems needs to be carefully planned to provide the desired operational result.

[7] It is the view of the project team that a CAD is a required element for a Public Safety Answering Point/911 center.

SECTION 3: REGULATORY CONTEXT AND IMPLICATIONS

ACS operation is impacted by a complex set of regulatory requirements. These regulatory and resulting compliance requirements come from federal, state, and/or local legislation, and necessitate a clear understanding of the requirements by the regulated party.

Regulatory requirements and facility-specific guidelines must always be considered in the specification, procurement, implementation, and maintenance of an ACS. ACSs need to comply with regulations such as 49 CFR § 1542 Airport Security and, where possible, should adhere to best practices such as US Customs and Border Protection's (CBP) *Airport Technical Design Standards*, RTCA DO-230J, and applicable International Electrotechnical Commission, American National Standards Institute, and Underwriters Laboratories (UL) standards. Additionally, airport operators must consider more general codes such as the National Electrical Code, as well as life safety codes such as National Fire Protection Association and local codes.

The regulatory environment related to PII, data privacy, and biometrics is complex and evolving rapidly. Section 6 of this guidance document discusses the issues and practical implications of these matters.

3.1 US Federal Regulations

US federal regulations are important drivers for how US airports design, procure, and deploy their ACSs. While federal regulations do not specify how an airport should provide access control or what, if any, technologies to use, they do establish functional requirements for an ACS (i.e., what it must be able to do).

In this section, we highlight some of the regulations from 49 CFR § 1542 that address airport security and designate TSA as the lead airport security regulatory authority.

3.1.1 Key Provisions of 49 CFR § 1542 (Airport Security)

49 CFR § 1542.101 establishes that covered airport operators must develop and maintain an ASP to provide for the safety and security of persons and property on an aircraft operating in air transportation or intrastate air transportation. It stipulates that all airport ASPs must be approved by TSA. Required ASP content is outlined in § 1542.103.

49 CFR § 1542.201 requires that as part of the ASP, covered airports must establish at least one Secured Area, and that each airport must prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into and within the Secured Area.

49 CFR § 1542.207 relates specifically to ACSs for covered airports. Its main provisions are:

- An airport must ensure that only those individuals authorized to have unescorted access to the Secured Area are able to gain entry;
- An individual must be immediately denied entry to a Secured Area when that person's access authority for that area is withdrawn; and
- An airport must provide means to differentiate between individuals authorized to have access to an entire Secured Area and individuals authorized access to only a particular portion of a Secured Area.

49 CFR § 1542.209 requires covered airports to conduct Criminal History Records Checks (CHRC) on all persons seeking unescorted access to an airport's SIDA and identifies a set of disqualifying criminal offenses.

49 CFR § 1542.211 relates to identification systems. Some of its key provisions include:

- Requirements for what information a personnel identification media must display;
- Requirements for how the personnel identification media must be worn; and
- Requirements for how an airport must ensure the accountability of all issued personnel identification, including the auditing of personnel identification.

3.1.2 US CBP Airport Technical Design Standards

While TSA is the lead federal regulatory agency for airport security, US international airports with Federal Inspection Station (FIS) facilities must also comply with CBP regulations, as outlined in the 2017 edition of US CBP's *Airport Technical Design Standards*.[8] CBP approval is required for credentials that allow access to FIS areas, and CBP requires that all credentials display a CBP access seal, typically in the form of an icon or hologram. Airports with FIS facilities or planning FIS facilities should request the current edition of *Airport Technical Design Standards* from CBP. The *Airport Technical Design Standards* is a controlled document, but is available upon request for airports that require and demonstrate a need to know.

3.2 State and Local Regulations

While it is beyond the scope of this guidance document to summarize all state and local regulations that may impact an airport ACS transition, it is important to highlight some general areas that airport managers should be aware of as they consider an ACS upgrade or transition:

- **Building and fire codes** – For example, these regulations will likely impact the types of doors and locks used by an airport as part of its ACS.
- **PII data protection regulations** – State and local governments may impose restrictions and regulations on the collection, disclosure, and protection of PII (see Section 6).
- **Credential approval** – According to RTCA DO-230J, some state and local authorities may require that approval for airport credentials be submitted to them in addition to the TSA.

3.3 Future Regulatory Trends

Federal, state, and local regulations can impact the design and operation of an airport ACS. Furthermore, regulations change over time, so it is desirable that a new or upgraded ACS have the capability to accommodate requirements resulting from future regulatory changes in a cost-effective and efficient manner.

Of course, predicting the exact nature and timing of future regulatory changes is difficult. Airport security regulations are often implemented in response to rapidly changing and emerging threats from bad actors who deliberately seek to surprise and be unpredictable. Through our literature review and interviews with subject matter experts, insider threat activity was identified as the most likely cause of further regulatory changes.

[8] US Customs and Border Patrol, *Airport Technical Design Standards*.

There are many historical examples of smuggling, industrial sabotage, and terrorism at US and international airports that involved aviation insiders (i.e., airport and airline employees and contractors). Incidents include:

- In 2019, a US airline mechanic sabotaged a navigation system of a 737-800 aircraft at Miami International Airport (MIA).
- In 2019, a flight attendant was arrested for allegedly smuggling drugs into Australia from Malaysia as part of a Vietnamese crime ring.
- In 2019, an individual linked to the al-Qaeda-linked al-Shabaab terrorist group was arrested in the Philippines while training to become a pilot, with probable nefarious intent.
- In 2018, at Seattle-Tacoma International Airport (SEA), an airline worker used his access to steal a Horizon Air passenger aircraft.
- In 2018, airline workers were arrested at Dallas-Fort Worth International Airport (DFW) for using their access to bypass airport security measures and smuggle drugs onto passenger aircraft.
- In 2017, federal government employees, airport security personnel, and a ramp employee smuggled cocaine through the TSA security system at San Juan Luis Muñoz Marín (SJU) Airport and onto commercial aircraft without detection.
- In 2016, an explosion occurred onboard a passenger aircraft traveling from Somalia. Somali intelligence officials say two airport workers handled a laptop containing a bomb that later exploded in the passenger aircraft.
- In 2014, at Hartsfield–Jackson Atlanta International Airport (ATL), an airport employee was arrested and charged with trafficking firearms and entering secure areas of a US airport in violation of security requirements.

In response to these incidents, TSA produced *Insider Threat Roadmap 2020*.[9] Though the TSA had developed previous insider threat documents and programs, this was the first formalized document released to the public outlining insider threat priorities. This document does not identify any planned or potential new TSA regulations. Instead, it emphasizes the importance of TSA and other aviation stakeholders, including airports, working together to increase the security baseline, sharing best practices, etc. For example, TSA's Insider Threat Roadmap states:

> "[TSA] will work with our security partners and stakeholders to understand the effectiveness of and improve on insider threat programs. [TSA] will seek to determine the level of compliance and governance needed for an organization to self-police."[10]

From this statement, it can be inferred that at some point in the future TSA may look to airports to support TSA's insider threat programs. The airport's ACS may provide useful data for that effort. For example, a relevant best practice identified in our research was for airports to periodically analyze their ACS data to determine if employees are in areas not related to their work. This may be a proactive way to identify patterns of behavior that represent a potential insider threat.

[9] Transportation Security Administration (TSA), *Insider Threat Roadmap 2020*, https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf
[10] Ibid., 11.

3.4 Implications for Airport ACS Transitions

Important considerations and takeaways related to ACS transitions can be drawn from this regulatory overview. First, airport ACSs are subject to airport-specific regulations and continual TSA regulatory oversight, which sets them apart from ACSs deployed in commercial office buildings, hospitals, or government facilities. Therefore, systems that work well in these non-airport environments may not be adequate for the requirements of a given airport, and experience and expertise in these non-airport ACSs may not translate to an airport operations environment. Parties involved in the design, selection, procurement, and integration of an airport ACS should have an adequate understanding of these regulations before beginning an ACS Transition Process.

In addition, TSA is a critical stakeholder and user of airport ACSs. TSA staff must rely on the airport ACS to perform their day-to-day tasks; therefore, their input as users should be taken into account during the ACS Transition Process. TSA staff are also often indirect users of the ACS in a broader sense. Airports use data from their ACSs to comply with TSA reporting and security audit purposes (e.g., to ensure that issued personnel identification is accounted for and being used appropriately). Thus, an airport ACS needs to support several TSA-driven regulations, and reporting and compliance requirements.

Finally, airport managers should conduct an assessment of regulatory requirements and guidelines that could impact one or more aspects of an ACS transition and ensure effective planning to meet those and any resulting compliance or reporting requirements. An example of how regulations can impact an ACS transition that was cited in our research was that when replacing an ACS, the airport must plan for guard posting at doors when the ACS is temporarily off-line during device replacement.

SECTION 4: AIRPORT ACS TRANSITION PROCESS: OVERVIEW, CONSIDERATIONS, AND BEST PRACTICES

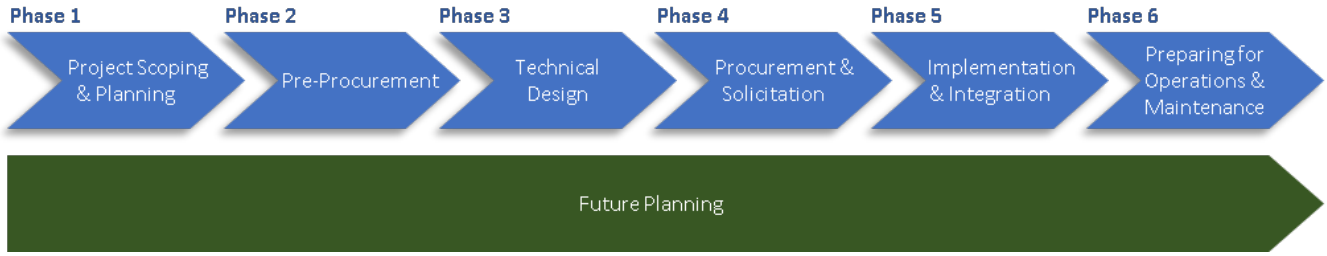
As discussed in Section 1, many airport ACS transitions follow a common pattern of activity that can be defined as a series of logically connected steps or phases. The ACS Transition Process can be generalized and divided into seven phases, as illustrated in Figure 8 below. It is recognized that there may be significant differences among airports in terms of specific requirements, sequencing of activities, or differences related to which activities fall into which process phase. However, the ACS Transition Process offers a flexible framework to support airport planning and initiation of an airport ACS upgrade or replacement.

In this section, we introduce the ACS Transition Process framework and provide a detailed discussion related to each of the seven distinct phases in the framework. For each phase, we present the following information:

1. A description or definition of each phase and the activities that occur within it
2. Considerations, best practices, and lessons learned associated with each phase
3. Process checklists for each phase

The information presented is based on interviews with airport subject matter experts and a literature review. By organizing information by process phase, airports can more easily plan for and initiate an ACS transition. The checklists are intended to help airports successfully accomplish the work within each ACS Transition Process Phase.

Figure 6. ACS Transition Process



4.1 Phase 1: Project Scoping and Planning

Airport ACS components are generally very reliable. It is not uncommon for the main hardware components of an ACS to operate and to be supported by ACS vendors for long periods of time, even as the system headend and software evolves. Some airports are operating ACSs that have been in place for decades, with equipment dating back to the original installation. As a result, it is often a daunting task to significantly upgrade or replace the existing system. This is why the Project Scoping and Planning phase is important.

The Project Scoping and Planning phase is the initial phase in the ACS Transition Process. It defines the key issues and questions to be answered before an ACS transition is started, and establishes the general parameters of the overall effort. This phase includes an assessment of the existing ACS relative to technology "end-of-life" considerations, as well as security, regulatory, and operational considerations. In this phase, activities also focus on gathering data to support a decision-making process for moving forward to the Pre-Procurement and Technical Design phases, which often require a significant investment of time and a broader application of planning resources.

This phase seeks to inform discussions related to the following questions:

- Are there sufficiently compelling reasons to ***consider*** upgrading or replacing the ACS?
- What are the realistic options available for consideration (e.g., is an upgrade a realistic option, or is a replacement needed)?
- What are Rough Order of Magnitude estimates of effort (in dollars, time, and opportunity cost) for upgrade versus replacement?
- What funding sources are available for the project?
- Is the necessary documentation available for the current system, including as-builts, to inform decisions during the design and transition processes?
- What procurement strategies are available for the project?

Outcome: Master Plan or Needs Assessment, and Preliminary System Requirements Document that informs pre-procurement activities.

Based on the results of evaluations during this phase, the airport may decide to proceed to the next phase of the ACS Transition Process. The Project Scoping and Planning phase would typically conclude with the mobilization of a small project team or project manager charged with gathering more detailed requirements, budgets, and project work plans.

The output of the Project Scoping and Planning phase is a Master Plan or Needs Assessment, and a Preliminary System Requirements Document that informs the Pre-Procurement phase of the project and serves as a foundational document for decision-making moving forward.

While a wide variety of planning processes were used by the surveyed airports, all concurred that scoping and planning was a critical step in the ACS Transition Process. Planning efforts allow the airport to effectively define the baseline requirements for the ACS project. The Project Scoping and Planning phase should include the following:

MASTER PLAN OR NEEDS ASSESSMENT

The creation of the Master Plan or Needs Assessment allows airports to review the overall system status, define system and user requirements, and identify relevant stakeholders. The Master Plan could be an overarching Information Technology/Low Voltage System Master Plan, or a more focused Security Master Plan or ACS Needs Assessment. If a Security Master Plan is created, it should include a framework of the airport's overall security program that maps operational, technical, and regulatory requirements for the ACS. For any Master Plan, the existing environment and a desired future environment should be clearly mapped and defined.

DOCUMENT EXISTING ENVIRONMENT

Mapping and documenting the as-is environment is important, as it helps identify requirements for the ACS. When defining the as-is state, it is important to carefully document the existing security environment and all of the systems that will be integrated with the ACS. If the airport has other security systems in place (e.g., IDMS, PSIM, CBT, DAC provider, etc.), ACS transition requirements can be impacted by the various integrations, where specific data will be stored, and how the system will be monitored.

CONDUCT MARKET SURVEY

A market survey should be performed to review the various access control vendor offerings, and available and emerging technologies. Market surveys help airports determine the current state of the ACS marketplace. By gathering this information in the planning stage, airport stakeholders can more clearly articulate their requirements during the procurement process.

PERFORM BUDGET REVIEW

Defining project budgets and ensuring that funding is available during the Project Scoping and Planning phase can help airports avoid delays and interruptions during latter phases of the process. Ensuring that the scope of the project is fully defined and complete will minimize changes over the course of the project and reduce the need for additional funding requests.

IDENTIFY SYSTEM STAKEHOLDERS

It is critical to identify system stakeholders early in the process and ensure their participation in the Project Scoping and Planning phase. Stakeholder identification efforts should be robust and consider all potentially impacted organizations and end users. It is important to facilitate clear, unambiguous communication between the stakeholders and all participants during this phase. This includes the entities that monitor the systems, and the end users that will be impacted by changes to the ACS, such as credential holders and credentialing office personnel.

ANALYZE AVAILABLE PROCUREMENT STRATEGIES

Understanding what procurement strategies are available to support the project will ensure that future decision-making is informed, and that limitations in terms of procurement are understood upfront.

Table 1. Project Scoping and Planning Checklist

Project Scoping and Planning Checklist		
Master Plan/Needs Assessment	Provide a Master Plan or Needs Assessment that:	
	• Defines the objectives for the ACS replacement or upgrade project	
	• Defines the operational, technical, and regulatory requirements for the ACS	
	• Defines the existing state of the ACS and the desired future state of the ACS	
Existing Environment	The existing environment should be documented to ensure that:	
	• All access control points are documented	
	• As-built documentation is accurate and complete	
	• All integrations are documented as part of the ACS replacement	
Market Survey	A Market Survey may be needed to review the current technology options that would be desired as part of the ACS future state.	
Budgeting	A budgeting exercise should be performed to identify the full scope of the work required and to ensure that all aspects of the project can be funded. The following costs considerations should be included:	
	ACS costs including:	
	○ ACS headend software	
	○ ACS licensing	
	○ Database licensing	
	○ Workstation and peripherals	
	○ Workstation licensing	
	○ Credentialing equipment and supplies	

Project Scoping and Planning Checklist		
	▪ Credential printers and encoders	
	▪ Security/holographic overlay	
	▪ Blank credential stock	
	○ Other IT costs such as virtualization licensing	
	○ ACS field equipment costs	
	▪ Card reader upgrade/replacement	
	▪ Card readers with biometric	
	▪ Request-to-exit (REX) devices	
	▪ Door position switch/monitoring	
	▪ Audible/visual devices	
	▪ Reset switches	
	▪ Door cabling and conduit	
	▪ ACS power supplies	
	▪ Door interface box	
	▪ Door hold open devices	
	▪ Anti-tailgating equipment/anti-piggy-backing equipment	
	▪ Automated, secure exit lanes	
	▪ Turnstiles/sally ports/security portals	
	▪ Other devices (list)	
	○ ACS cabling and conduit from door to communication room	
	○ Door/reader interface panels	
	○ Intelligent field panels	
	• Vehicle gate improvements	
	○ Card readers upgrades	
	○ Card reader pedestal upgrades	
	○ Gate operator upgrades/replacements	
	○ Gate position switch upgrades	
	○ Gate audible/visual devices	
	○ Gate safety equipment upgrades/replacements	
	▪ Gate safety edge equipment	
	▪ Vehicle detection loops	
	▪ Photo eye sensors	
	▪ Other	
	○ Gate equipment panel replacement/upgrades	

Project Scoping and Planning Checklist		
	▪ Equipment enclosure replacement	
	▪ Cooling/heating equipment for enclosure	
	▪ Upgrade to ACS equipment in enclosure	
	○ Upgrade to conduit/cabling at gate	
	○ ACS power supplies	
	○ Civil works upgrades to pavement/curbs	
	○ Gate hardening (crash rating if applicable)	
	○ Protection equipment (bollards, barriers, etc.)	
	○ Traffic control equipment	
	• Mechanical system improvements	
	○ Heating/cooling upgrades	
	○ Humidity control	
	• Electrical power and UPS improvements	
	○ Add electrical capacity/panels	
	○ Add circuits/breakers	
	○ Add dedicated outlets/circuits	
	○ Add UPS units/batteries to support ACS	
	○ Add UPS units to support ACS support equipment, including LAN, communications, etc.	
	• Architectural upgrades	
	○ Door upgrades/replacement	
	▪ Swing/bi-fold doors	
	▪ Sliding doors (powered and manually operated)	
	▪ Security revolving doors (powered and manually operated)	
	▪ Automated secure exit lanes	
	▪ Security portals/sally ports/man traps	
	▪ Turnstiles	
	▪ Other door types	
	○ Door hardware upgrades/replacement	
	▪ Electrified locking devices	
	▪ Egress/panic hardware	
	▪ Delayed egress equipment	
	▪ Power transfer devices	
	▪ Door closer equipment	

Project Scoping and Planning Checklist		
	▪ Door power operators	
	▪ Door hold open devices	
	○ Other upgrades at doors such as reader pedestals, ADA compliance equipment such as handrails, etc.	
	• Communication system upgrades as needed to support the ACS	
	○ Network switch upgrades/replacement/additions	
	○ Network uplink upgrades	
	○ Core/distribution switch upgrades	
	○ Wireless link upgrades/replacement/upgrades (if applicable)	
	○ Additional communication system upgrades as needed	
	• IT infrastructure upgrades	
	○ Backbone fiber	
	○ Backbone copper	
	○ ISP/internet access upgrades	
	• Other systems that may need to be upgraded, revise, or otherwise enhanced as part of the overall security project	
	○ CCTV/VSS	
	○ Fire alarm system	
	○ Credentialing/identity management (if separate from ACS)	
	○ PSIM (if applicable)	
	○ CBT	
	○ DAC service	
	○ CAD (if applicable)	
	○ Other	
System Stakeholders	Identify major stakeholders in the ACS, which could include:	
	• Airport security	
	• Airport operations	
	• Credentialing personnel	
	• ACS system operators	
	• Airport police/security personnel	
	• Airport fire personnel/authority having jurisdiction (AHJ)	
	• Airport tenants	
	• TSA	
	• CBP	

Project Scoping and Planning Checklist		
	• Airport leadership, including any board, city, county, and state personnel	
	• Other	
Analysis of Procurement Strategies	Identify procurement strategies that are available for the project and any potential limitations or requirements that exist for procurement efforts	

4.2 Phase 2: Pre-Procurement

The Pre-Procurement phase should build on the work performed during the Project Scoping and Planning phase. This phase primarily focuses on requirements gathering, stakeholder engagement, and project planning and approvals. Outputs from this phase will inform the system design, and ensure it is complete.

The Pre-Procurement phase seeks to inform discussions related to the following questions:

- What are the needs and requirements of the ACS stakeholders and end users, and how will the transition impact them?
- What are the specific capabilities or features that are needed in an ACS, and have they been documented?

Outcome: Final System Requirements Document that contains informed requirements that represent the needs of a broad set of airport community stakeholders

It is typically during this phase that upgrading or replacing an ACS shifts from being an idea under consideration to a project with assigned resources, a preliminary budget and timeline, and at least conditional approval by senior airport management. An airport will also define and critically evaluate the potential alternative ACS transition approaches during this phase. The Pre-Procurement phase should include the following:

FINALIZE DECISION TO UPGRADE VS. REPLACE EXISTING SYSTEM

There are a variety of factors to consider when determining whether to upgrade or replace an ACS. This decision should consider cost as well as an evaluation of the current system and its end-of-life horizon. While an upgrade may appear to be the fiscally sound choice, it may necessitate upgrading all components (field panels, readers, infrastructure, etc.), which could cost more than a system replacement. Other factors include the support and ongoing costs for the system. Support structure and pricing varies from vendor to vendor; a lower cost for ongoing support and licensing fees or the ability to have multiple integrators bid on additional work can be major factors in whether to pursue alternate systems.

- **IT Requirements –** ACSs have become much more IT-centric over the past decade, and the ability to leverage the existing IT infrastructure, including the Local Area Network (LAN), use of Power over Ethernet (PoE), and the server and storage infrastructure are major considerations. As the maintenance of these systems becomes more focused on IT, the more aligned these systems need to be with the overall IT objectives and standards of the system stakeholders, including Airport IT and Airport Security, as well as users of the system such as Airport Police and CBP/DHS.
- **Existing Infrastructure –** The ability to use the existing infrastructure, such as the LAN, storage, and virtualized server environment, as well as using more standardized IT type horizontal cabling, will allow for easier management and maintenance of the ACS.

- **Stakeholder Needs –** When starting a replacement project, it is important to begin by gathering the stakeholder needs and wants, as well as understanding the current operational and regulatory requirements specific to the facility. Once the needs of the various groups are gathered, the requirements should be reviewed and classified as regulatory requirements, operational requirements, or user-requested items.
- **Integration with Existing Systems (e.g., IDMS, VSS) –** It is common that the minimum requirement for an ACS is the ability to be integrated with a traditional system, such as an IDMS for the creation of access control users, credentials, and access rights, or with a VSS for camera call-up upon alarm.
- **Cost/Benefit Analysis –** The cost/benefit analysis will typically include the initial cost to upgrade or replace the existing system, as well as the ongoing licensing, maintenance, and support costs to allow for a total cost of ownership evaluation.

GATHER STAKEHOLDER INPUT

Airports should consider the input and feedback of all impacted end users and stakeholders as part of the system design. During the Pre-Procurement phase, the airport has primary responsibility for identifying stakeholders and defining the role that each stakeholder has during the procurement. Some stakeholders will be considered minor system users, while others may be equal partners who have significant input for final system outcomes.

ASSEMBLE WORKING GROUPS

The airport should consider creating working groups with the major partners impacted by the ACS. This is especially important for airports that have external organizations that are directly involved in the operation of the airport, such as those operated by city or state agencies. In such cases, these agencies are often directly involved with the airport systems, or may oversee operational or administrative aspects of the systems. For example, airports that are managed by city municipalities should consider forming a working group with city management, so they are aware of and understand the project and system requirements. Making them part of the key stakeholder group at the beginning of the project will smooth the process and ensure that they are familiar with the project, understand the objectives, and feel comfortable that their needs will be met as part of the implementation. Establishing such working groups also helps users feel invested in the success of the project, and helps to establish shared timelines for the project.

DETERMINE SYSTEM REQUIREMENTS

Airports should ensure that they have developed thorough requirements, and that system features that are considered during the transition process are fully understood. The requirements will define what the ACS will do to meet the needs of the stakeholders, but not how the system will do it. Clear requirements must be concise, feasible, testable, and unambiguous. Instead of focusing on the capabilities of each manufacturer, the specifications should note the required capabilities in a product-agnostic fashion.

> Often vendor specification and contract documents will note that the system shall be capable of the required features and capabilities. However, features and capabilities that are not specifically required are sometimes excluded from the vendor agreement. This can lead to change orders and unanticipated expenses.
>
> It is important to understand all of a system's features to help ensure they can be fully implemented. If they are not understood and used at the outset, this may lead to a poor operational outcome and dissatisfaction with the system. In addition, having features or modules that are not actively used may cause the airport to incur unnecessary costs.

Items that are often overlooked in planning and budgeting an ACS upgrade or replacement can include extended warranties, maintenance programs, maintaining as-builts, accommodations for future expandability, and personnel costs for guarding unsecured zones during installation, construction, and transition. These may lead to long-term expenses that were not originally planned.

Understanding what is included and using those features or modules to the fullest extent ensures proper operation, optimal system capability, and the robust realization of the benefits offered by the system procured.

DOCUMENT DECISIONS

It is critical that airports carefully document the decisions that are made in this phase. Important documentation material includes meeting minutes, a listing of requirements, market research, and other planning and design work performed during the planning process. The requirements should be consolidated and defined in a decision matrix that documents the disposition of each request. Formalizing the documentation process for stakeholder identification and decision-making allows consistency throughout the project, and can help avoid revisiting earlier decisions in later phases.

If a documented request is to be included as a requirement, then it should be prioritized in the list of project requirements. If a documented request is to be excluded, a list of the pros and cons should be documented with the decision and the final reason for not including the item in the procurement. This will allow for the decisions made in the design process to be justified and explained in the future.

The prioritized listing of requirements in a matrix is a useful tool during procurement and implementation. For example, if a manufacturer takes exception to a requirement, this prioritized listing will allow the airport to determine if the exception represents a major or minor requirement and then proceed accordingly. In addition, the matrix allows for verification of the stakeholder requirements, allowing the airport to confirm the acceptability of any exceptions with the specific stakeholders prior to accepting or rejecting the change.

Table 2. Pre-Procurement Scope Checklist

Pre-Procurement Scope Checklist		
Stakeholder Input	Based on the stakeholders defined in the Project Scoping and Planning phase, input should be sought from the stakeholders regarding:	
	• ACS security requirements/enhancements	
	• ACS operational enhancements	
	• ACS regulatory changes	
	• Code changes that could impact the ACS replacement (National Fire Protection Association, IBC, etc.)	
	• ACS replacement schedule and phasing	
	• Changes to end-user interface with ACS	
	• Changes to credentialing process (if applicable)	

	• Training requirements	
	• Other	
Establish Working Groups	Create working groups to allow for gathering of desired features, functions, and requirements:	
	• Leadership group	
	• Security/Regulatory group	
	• Operational group	
	• Code Compliance group	
	• Major Airport Tenant group	
	• Other groups	
Documentation of Decisions	As part of the working group sessions, it is important to document the input from the working groups. It is recommended that a matrix be created to include the following information:	
	• Specific feature or capability requested	
	• Group(s) requesting feature or capability	
	• Nature of request:	
	○ Code/regulatory requirement	
	○ Operational requirement	
	○ User requests	
	○ Business enhancement	
	• Disposition of requirement/request	
	○ To be included as mandatory	
	○ To be included as optional/nice to have	
	○ Not to be included	

4.3 Phase 3: Technical Design

Once the Pre-Procurement phase is completed, the airport may move into the Technical Design phase. This step allows airports to create a technical design of the ACS that will support procurement, installation, testing, and quality assurance activities throughout the transition process. Transition to the Technical Design phase assumes that funding is available and that the scope of the project has been clearly defined.

In this phase (which often involves the use of an outside consultant or ACS design firm), the objective is to produce a design that defines the airport's desired technical end-stage, and that can be shared with outside firms as part of the solicitation and procurement process. The phase can vary depending upon the type of procurement vehicle that the airport expects to use for the project, as this could impact the process used and the parties that need to be involved.

This phase seeks to answer the following questions:

- Is a design firm needed or is there in-house expertise to support the project?
- If using a design firm, does the identified firm have the necessary airport-specific experience to meet the needs of the project?
- Does the ACS need to be scaled for inclusion of additional systems or access points?
- Does the existing infrastructure support the IT and system requirements for the new ACS or will upgrades be needed?
- Will upgrades to other systems be required as a result of the installation of the new or upgraded ACS?
- Have the required features identified in the Pre-Procurement phase been incorporated into the design?

Outcome: Source-selection factors that support defined system requirements and ensure success of the project during implementation, integration, and beyond.

Contributing airports noted that conducting an adequate Technical Design is a critical step. Regardless of the procurement type used for the ACS replacement or upgrade, some level of design is necessary to ensure that the scope of work is clearly defined to allow for the bids or proposals to be thoroughly and substantively compared. The Technical Design phase should address the following at a minimum:

DESIGN FIRM QUALIFICATIONS

Selecting a firm to provide the design for the ACS is an important part of the Technical Design phase. For a procurement that will be bid, it is recommended that a design firm be retained to provide a basis of bid, or a complete design based upon the procurement methodology selected. In reviewing potential ACS designers, airports should ensure that the design firm has substantial experience in the design of airport-specific ACSs and a thorough understanding of airport operations. Design firms should have requisite knowledge of and experience working within the airport regulatory environment. They should possess a thorough understanding of the specific operational needs of the airport, and be mindful of ACS requirements of entities such as CBP and TSA. Airports have unique regulatory and security requirements compared to non-aviation facilities that also use ACS. These aviation-specific requirements will need to be reflected as a major portion of the design. In addition, design firms with a depth of experience in the airport environment will typically understand the differences in the operational and business practices, and will be able to provide a design that meets the requirements for the airport.

The need for an experienced design firm was mentioned numerous times among the airports that were interviewed, with many airports noting pitfalls that occurred due to a lack of airport-specific experience. The pitfalls included designs that did not meet the airport's complex operating requirements, necessitated change orders, and in many cases required the airport to take a much more active role in the design and construction process. This often caused extensive work for airport personnel in addition to their regular job duties, and caused delays to the schedule, resulting in the project being completed late and over the allocated budget.

SYSTEM FEATURES

The required features of the ACS will need to be guided by the current and/or planned airport environment. If the airport has an existing IDMS, CAD, or PSIM[11] system, or intends to procure any of

[11] PSIM is a category of software that is designed to integrate multiple unconnected security applications, enable automation of workflows and processes, and to provide control over devices through a unified user experience.

these in conjunction with its ACS transition project, then the features required in the ACS, such as a credentialing function or GUI, may be minimal. However, if these systems do not exist and are not specifically included as part of the ACS transition project, then the ACS will need to include these capabilities, and the requirements will need to be carefully defined to meet the needs of the airport. In addition, the transition planning will need to include the creation or transition of data such as the cardholder database, based on what is included in the ACS features. The system features should be informed by the market survey, stakeholder requirements, and the system requirements as documented during the previous phases of the project.

OPERATIONAL CONSIDERATIONS

The Technical Design phase should include thorough consideration of the operational and security procedures and practices employed at the airport, as these processes and procedures will drive user interaction with the ACS, and the system will need to fully support those user interactions and requirements. In order to successfully support operational requirements, the system will need to provide the proper data storage, presentation, and reporting capabilities, and include the interfaces and integrations to push or pull data from other systems that are part of the overall security operation. It is critical to capture these processes and procedures as part of the Technical Design phase, and ensure that the design includes elements to support these processes.

SYSTEM DEPLOYMENT PLANS

The Technical Design phase also provides an opportunity to review the system deployment plans. These typically consist of the ACS objectives and the existing system plans. Many airports have developed and documented system objectives, often in the form of a matrix, that define the security boundaries and the expected ACS measures for passing between the airport security zones. For airports that have not formally documented the ACS objectives, the Technical Design phase provides the opportunity to do so. The objectives for the ACS should be reviewed and validated, and it should be determined whether the existing system deployment is appropriate, or if doors should be added or deleted as part of the replacement or upgrade.

The deployment plans should also include planning for training, dual system operation, database transition, and system testing. The deployment plan should address all of these items at a high level and set the minimum requirements. Refer to Section 4.5 for further information.

> As the regulatory environment evolves, additional access points may be required, or portals may need to be minimized. Egress requirements may have changed due to changes in code and aircraft capacity. All of these factors should be considered in the planning and design of the ACS rather than just proceeding with a one-for-one replacement.

AIRPORT INFRASTRUCTURE

As ACSs have matured, they have become more network-centric. This requires airports to ensure that the network infrastructure can support the ACS replacement. For example, it is not uncommon that older systems were implemented using legacy communications such as serial communication.

The location of the equipment should also be considered, as there are many cases where the existing deployment may have negative impacts. For example, equipment that supports a portal may be located in boxes above the portal. While this is acceptable, safety and security protocols often make servicing these devices very difficult during airport operational hours, or may require that the service be performed during overnight hours, thus removing portals from use until the next available maintenance window.

These considerations may necessitate a different application of equipment and cabling, which could impact the location of equipment or modify the cabling that is used to connect the portal equipment. With the advent of network-connected interface panels and the use of PoE, the cabling requirements have the potential to change substantially. Similarly, the distance that is allowable from the portal to the communication room may be limited to the 100-meter distance typical for network cabling. These factors could drive the need for additional infrastructure or communication room locations to support the updated system. Moreover, the implementation of additional backbone fiber, network equipment, emergency power, and/or UPS units may be required as part of the system deployment. If the existing system has legacy cabling or communication means in place, and if the airport wants to maintain the existing legacy cabling, reusing the existing cabling or communications means may require a different architecture that is compatible with the existing installation instead of using a generic approach. Regardless of the situation, the unique needs of the airport should be assessed, and the chosen design approach should enable implementation of the system without requiring change orders to address issues that were not anticipated as part of the design.

PHYSICAL UPGRADES

When planning the replacement of an ACS, it is important to consider the full system environment that is impacted by the ACS. While the primary focus of the Technical Design is typically the ACS and the associated hardware such as card readers, the ACS is ultimately dependent upon the proper operation of the doors and gates to which it is applied; therefore, consideration of these points is critical. If the doors or gates do not operate properly, do not close well, or have outdated hardware, the ACS may experience issues such as false alarms and system errors. In addition, the current access control points should be reviewed for possible future needs, such as the potential need for higher security requirements, anticipated changes in staffing such as the need to remove TSA personnel or guards, or changes that could require additional tracking of credentialed personnel to enforce policies or procedures, such as to prevent or detect security violations like piggybacking/tailgating.

> In many cases, the replacement of access control point components such as portals, sallyports, turnstiles, doors, gates, gate operators, and door hardware should be considered as part of the system replacement. The typical issues include doors not operating correctly and doors lacking proper weather sealing, which may cause long-term maintenance issues with the ACS equipment.

As part of any door replacement project, the upgrades or changes to the door hardware should be considered as part of the system upgrade. These changes may include replacing legacy door hardware with newer versions, which may include additional features, door hardware that aligns with the safety and egress code requirements, and door hardware that draws less power, which can minimize the electrical consumption of the ACS. Reducing power requirements could potentially allow for a reduction in battery and/or UPS capacity required to support the system. See Section 5.5 for more information on door hardware options.

Secured Area perimeter gates could encompass pedestrian gates or vehicle gates, and could include the replacement of the physical gate/turnstile, operators, or the equipment cabinet, or the addition of safety hardware and associated equipment such as pedestals, bollards, etc.

In addition, other security enhancements may be deemed necessary as part of the physical upgrades. These could include the provision of security revolving doors, turnstiles with special features such as full height barriers and crawl detection, or automated secure exit lane technology to enable or enhance unmanned security entrances and exits.

DEVICE NAMING

As part of the Technical Design Phase, consideration should be given to device naming within the ACS. There are several strategies that can be employed to name the devices, and many are directly related to the facility naming conventions. For an ACS, there are typically two or more pieces of data given to each portal, gate, or point on the system. The first is the name for the device within the system, which is often limited in length and is displayed on maps and in the system alarm monitoring window. Additional data may include device type (reader, input point such as door position switch, output such as audio-visual, lock, etc.), the device location, and other data as allowed by the system to define the device.

Even if the system allows for long names, it is desirable to provide the system operators with a short name that they can easily remember, and then provide a longer descriptor of the point location. Most facilities have a naming convention that is based on the physical location of the device, and provides basic location data that can be quickly decoded. The following is a possible example of a naming convention that could be used at an airport:

SS-FF-LL-XXX

SS – Site associated with the point. For an ACS that is implemented for a single site, this may not be necessary, but if a system is implemented across multiple airports, then this would define the specific airport.

FF – Facility associated with the ACS point. For example, this could include items such as:

T1 – Terminal 1
AR – ARFF
CT – Control Tower

LL – Level Associated with the ACS point. For example, this could include:

B – Basement
1 – First Floor
U – Upper Level

XXX – Unique Identifier associated with the ACS point. For example, this could include:

001 – Sequential numbering of all devices with the specific facility and level
G01 – Naming by the gate or area associated with the ACS point

The intent is to provide a usable naming convention for system operators so that they can more easily recognize the point and memorize the location. For example, if a point is named CA-UL-BD05, the operators will immediately know that the alarm is on Concourse A, on the Upper Level, for the Boarding Door at Gate 5, and can dispatch without needing to reference the longer description. Or, if an alarm is received for T1-LL-CR05, the operator would know that the Terminal 1 Lower Level Communication Room 05 has an alarm.

Regardless of the naming convention used, it is recommended that the names and descriptions be confirmed by the airport and the ACS operators prior to programming them into the system. See Phase 5 (Section 4.5) for more details.

NON-PROPRIETARY SYSTEM EQUIPMENT

Many airports desire to have non-proprietary equipment as part of the ACS replacement. This allows for the system headend to be replaced while maintaining the existing field equipment. Non-proprietary

equipment allows for changes should issues arise with the integrator or manufacturer. This is a particular concern if the available integrators for a specific manufacturer are limited in the area where the airport is located.

LEVEL OF SYSTEM INTEGRATION

The level of integration between the ACS and external systems will impact the interaction between the various systems and their maintenance strategies.

In cases where an airport has systems such as IDMS and/or PSIM/CAD systems similar to the integration shown in Figure 5, ACS Integrated to PSIM (Section 2.2.4), the integration of the ACS may be limited to the PSIM/CAD and the IDMS. In this scenario, the ACS user interface would not be used as the primary interaction with the system, as the primary interface would be through the PSIM/CAD GUI. While their integration to the ACS may be more limited, the use of systems such as PSIM and IDMS will restrict upgrades to the ACS until they can be vetted and approved by the PSIM and IDMS manufacturer. In this regard, it should be considered that these systems will place limitations on possible upgrades and changes to the ACS, which may make the overall environment more complex to manage.

In cases where an airport has a separate IDMS but intends to use the ACS and/or VSS user interface as the GUI for monitoring the systems, the integration would be as shown in Figure 4, ACS Integrated to IDMS and VSS (Section 2.2.3). In this type of scenario, there are tight integrations and loose integrations. Tight integrations are typically designed to allow for a single user interface to be used to perform most of the systems' functions. In some cases, this tight integration is a design feature of a single manufacturer's product line, while in other cases the integration is due to an exclusive agreement between two different manufacturers.

At the opposite end of the spectrum, some airports prefer a loose integration between the ACS and other systems. In this scenario, the various systems would be monitored via their respective user interfaces. This typically means that operators will need to use multiple programs simultaneously, creating a more complex environment for the system operators. The systems would be integrated through industry-standard methodologies or Software Development Kit (SDK) integrations. Loose integrations have more limited capabilities, but are less sensitive to system changes on each side of the integration. There also will be more integration points to be maintained in this scenario, which may increase maintenance.

If an airport would like to procure an ACS with an integral credentialing application similar to the integration scenario represented in Figure 3, ACS with Integral Credentialing and Integrated to VSS, CBT, and DAC (Section 2.2.2), then the overall integration will be simplified, and will not have additional costs that are typically associated with a third-party IDMS. For many facilities, an ACS's integral credentialing may have sufficient capacity and capabilities to support the airport's credentialing processes. However, the process enforcement features typically found in an IDMS, as well as some of the more advanced integrations (e.g., DAC integrations offered by some IDMS systems), may not be available for the integral credentialing function.

An airport may find that there are a limited number of systems that can provide the desired level of integration, especially if attempting to maintain existing systems and only replace the ACS. This limits the available product combinations that can be considered, or could require that both the ACS and VSS be replaced simultaneously. For tightly integrated systems, the products chosen may commit the airport to the specific manufacturers for the foreseeable future. However, the implementation of tightly integrated systems will likely be more economical than a PSIM/CAD type of implementation, and would be easier for the operators to navigate than the loose integration approach. For tightly integrated systems, the compatibility of the integration will be ensured and managed by the manufacturers, which

will reduce the overall effort required by the airport to maintain the system integrations. So, while tied to the products, it will likely be easier to manage than multiple loose integrations.

While any of these approaches may be considered, it is important to weigh the pros and cons of each as part of the system planning, and determine the best fit for the airport based on the specific environment, financial impacts, and support capabilities at each facility.

Table 3. Technical Design Scope Checklist

Technical Design Scope Checklist		
Design Firm Qualifications	Qualifications should include:	
	• Airport-specific security design experience	
	• Experience with the regulatory environment of an airport including:	
	○ Airport operational requirements	
	○ TSA regulations and requirements	
	○ CBP regulations and requirements	
	• Experience with airport credentialing requirements	
System Features	The desired system features that were identified as part of the previous phases should be used to inform the design, including:	
	• Master Plan elements	
	• Technologies identified as part of the Market Survey	
	• Documentation on the existing environment, including other systems to be integrated with the ACS	
	• Matrix of decisions should be used to guide the features to be provided	
Operational Considerations	Consider the operational and security procedures and practices at the airport	
System Deployment Plans	The design of the ACS affords the opportunity to review:	
	• Current deployment to determine if existing doors should be maintained	
	• Potential need for ACS expansion	
	• Additional opportunities for the use of the ACS	
Airport Infrastructure	If infrastructure upgrades are needed to support the ACS, the Technical Design should include:	
	• Backbone infrastructure upgrades	
	• Communication room upgrades	
	• IT equipment upgrades (network switches, etc.)	
Physical Upgrades	Physical upgrades may include:	
	• Door upgrades/replacements	
	• Door hardware upgrades/replacements	
	• Pedestrian/vehicle gate upgrades/replacements	

Device Naming	Determine naming convention to be employed for devices and access points	
Non-Proprietary System Equipment	Determine whether non-proprietary system equipment is preferable	
Level of System Integration	Determine desired level of integration between the ACS and external systems (i.e., integral, tightly integrated, loose integration)	
	• IDMS	
	• VSS	
	• DAC	
	• CBT	

4.4 Phase 4: Procurement and Solicitation

In the Procurement and Solicitation phase, the objective is to establish a procurement approach, and select a contractor/integrator to implement the desired technical design and support the ACS Transition Process (i.e., will a security system integrator be used? Will the airport contract directly with the ACS vendor?) This phase is usually heavily influenced and driven by a range of stakeholders, organizational dynamics, and processes that include but can extend beyond airport ACS operations. This can make Procurement and Solicitation a particularly complex and time-consuming phase for any ACS transition.

This phase seeks to inform discussions related to the following questions:

- What procurement methodologies are available and which is best for the project?
- Does the solicitation for contractors include requirements for airport-specific experience and demonstrated past performance with similar projects?
- Does a contractor with a local presence need to be included to support activities over the life cycle of the project and post-implementation?

Outcome: Selection of an experienced contractor/integrator with relevant past performance that understands the airport's goals and needs for the ACS transition.

CONFIRM THE PROCUREMENT STRATEGY

The procurement methodology chosen by an airport will be highly dependent upon the rules and regulations that apply for procurements at their facility. Most US commercial airports are either a public authority or part of a local or state government. In either case, they are accountable to local officials and local taxpayers. In many instances, a solicitation for an ACS cannot even be initiated without prior legal and, in some cases, legislative approval. Furthermore, in many cases, the procurement process is managed by a dedicated procurement department. The procurement type and process should account for all of the possible restrictions and requirements identified for the airport, as well as the funding mechanisms that will be used for the project. The relative advantages of different procurement methods should be considered to ensure that the airport has the most flexibility possible in the selection of the system and the contractor/integrator.

Examples of procurement methodologies are:

1. **Design-Bid-Build –** The traditional approach in which a full design is provided, followed by a public procurement with multiple bids. The winning bid is the lowest cost bid deemed to be responsive and in compliance with the contract documents.

2. **Design/Build Procurement –** The Design/Build procurement will typically provide a preliminary design document that allows for the design/build teams to determine the expected costs to complete the system design and provide the system replacement. The design/build team can include a design firm that is brought on as part of the team, or it can include a set cost to utilize the airport's designer as part of the design/build team. The lowest bid is typically deemed the winning bid. Once awarded, the design/build team will begin the implementation while also completing the design in parallel. This may reduce the overall project duration and may be attractive for fast-track project timelines.
3. **Best Value Procurement –** Best Value procurement is similar to Design-Bid-Build, but in this case the airport can review multiple factors of the bid, with price being only one factor. In this type of procurement, the lowest bid may not be selected based on other factors that are used as part of the selection.
4. **Request for Qualifications (RFQ)-Request for Proposals (RFP) Procurement –** The RFQ-RFP procurement is a two-step process that begins with the airport releasing an RFQ. The RFQ typically identifies minimum qualifications (including examples of experience with airport-specific ACS projects) and requests that interested teams submit their qualifications. For teams deemed to be qualified, the airport will issue an RFP, which the qualified teams will then use to provide a bid with pricing. The lowest bid submitted by the qualified teams typically wins.
5. **Sole Source Procurement –** Sole source procurements are relatively uncommon given the restrictions that many airports are subject to as publicly funded entities. However, a sole source procurement can be justified for direct upgrade types of projects, or if allowed by the airport.

The procurement methodology may also be dependent upon whether the project is considered an upgrade or replacement, as an upgrade could have different procurement rules associated with that approach. The procurement may also involve conducting pre-solicitation briefings or workshops for potential bidders.

ESTABLISH CONTRACTOR/INTEGRATOR REQUIREMENTS

The airport-specific experience of a contractor/integrator is of key importance. Airports operate differently from other types of facilities and have unique regulations affecting access control. The transition from legacy ACS to new or upgraded system will be better informed if the integrator and contractors have experience-based understanding of the airport environment's limitations and security requirements. For example, unlike other types of facilities, airport doors cannot be left unsecured at any time if the doors provide access to regulated areas. Implications of these types of requirements will need to be considered and planned for as part of the implementation process, and may result in an extended process or extra requirements, such as the need to provide security personnel to protect portals during cutover. These types of requirements will incur a cost, either directly or indirectly, and could result in delays or unnecessary change orders if they are not accounted for at the beginning of the process. The integrator's experience in airports will help to ensure that they include these factors in their bids.

The recommended qualifications for the manufacturer and integrator should include:

- Integrators should have at least three airport deployments of a similar size, with at least five years of experience at comparable airports acting as the security integrator under a construction manager or prime contractor, or acting as the prime contractor.
- Manufacturers should have experience with implementing the proposed system in at least three comparable airports in North America.

- As part of the proposal or bid, the integrator and manufacturer should provide a minimum of five references for the experience listed above, with at least one of those projects being the proposed system as implemented by the integrator.

The need for local integrator presence in the immediate vicinity of the airport should be considered. If the contractor is not located near the airport, their ability to respond in a timely manner (as potentially specified in the contractual Service Level Agreement) may be impacted. Many airports will require that the integrator office be within a specific distance of the airport, and that all responses to critical calls be subject to Service Level Agreements. In addition, it is important to specify and verify that the integrator is a certified reseller of the system and has multiple employees that are certified on the system by the manufacturer. Identifying multiple local integrators that are certified on the system allows for competitive bidding of construction and maintenance for the installed system, providing options and flexibility for future needs.

MAINTENANCE AND WARRANTY

It is common for the airport to require the basic warranty and maintenance period be included in the base bid. This typically includes a one-year warranty that is activated at the completion of system implementation. The airport may also request pricing for an extended warranty and maintenance contract. In many cases, the pricing will include three to five years of extended warranty and maintenance, and the airport will have until the end of system installation, or until the end of the basic warranty, to notify the integrator if the warranty and maintenance contract will be extended. System support and maintenance is discussed further in Section 4.6.2.

A majority of surveyed airports recommended that the initial procurement include a provision for the contractor/integrator to provide the first three to five years of system maintenance.

Table 4. Procurement and Solicitation Scope Checklist

Procurement and Solicitation Scope Checklist		
Procurement Methodology	Confirm procurement type to be selected based on the regulations and policies for the airport. Procurement type could include:	
	• Design-Bid Build	
	• Best Value Procurement	
	• RFQ-RFP Procurement	
	• Design-Build Procurement	
	• Sole Source Procurement	
Contractor/Integrator Experience	Contractor/Integrator experience should include the following:	
	• Experience working in the airport environment	
	• Experience working with the proposed system manufacturer, including being a certified reseller and having personnel certified on the system	
	• Experience and knowledge related to maintaining airport security requirements during construction	
Integrator Local Presence	Integrators should have a local presence near the airport, including:	
	• Local office within a specified distance	

	• Personnel able to respond within a preset length of time	
Maintenance and Warranty	Include terms for system maintenance and warranty	
	• Basic maintenance and warranty terms	
	• Extended maintenance and warranty terms and price	

4.5 Phase 5: Implementation and Integration

During the Integration and Implementation phase, the selected contractor installs the hardware, software, and other components purchased for the ACS upgrade or replacement, and performs integration with legacy systems such as VSS and IDMS. It may also be necessary to modify airport facilities through work such as new cable or power installation, and other construction modifications.

Depending on the size of the airport and the scope of the ACS transition, the airport may also need to plan for a phased implementation or cutover from their legacy ACS to their upgraded or replaced ACS, often by running the two systems in parallel for a period of time.

In addition, system testing is conducted against all system performance requirements and interfaces, all new ACS documentation is delivered, and training of system operators occurs.

This phase seeks to answer the following questions:

- Has ACS implementation and integration been appropriately phased?
- Has the ACS been successfully implemented and integrated with related airport systems?
- Has user acceptance testing of the system been completed?
- Has adequate training been provided to all system operators and end users and has follow-up training been planned as needed?
- If operating dual systems, are systems operating appropriately together and addressing all airport requirements?
- Has an end date been identified for the legacy ACS?

Outcome: Successful integration and installation of the ACS without inadvertent loss of access control functionality.

The implementation of an airport ACS is a phase in which major financial and operational investments are often required, so ensuring its success is critical. By pre-planning implementation steps and accounting for the individual stages, the airport will be able to create a roadmap for completion and ensure proper scheduling for the system replacement. In addition, the sequencing of the ACS implementation will help to inform stakeholders and system users who will be impacted at any given time to allow for advance coordination to minimize possible disruption.

As part of the system implementation, the naming of devices within the system and the labeling and identification of all of the ACS portals, doors, components, conduit, and cabling is critical. For additional information, see Section 4.3, as well as the RTCA Standards for Airport Security Access Control Systems (RTCA DO-230J) and other industry guidance documents.

It is recommended that the system installer provide a submittal with a listing of the ACS point names and the logical descriptions for airport approval. This will allow for a final confirmation by the airport to make sure that they are happy with the information to be programmed into the system. This also allows for the system installer to revise any names based on changes in the original contract documents, as well

as revise any naming conventions based on possible limitations of the ACS system being installed. For example, if the quantity of characters is limited or special characters such as dashes cannot be used, the installer can present revised names for airport approval.

The following activities should be considered as part of the Implementation and Integration phase. While this is not an exhaustive list, these activities can be used as a guide to ensure that the critical actions are considered in planning. During these activities, it is important to ensure that security requirements are adhered to at all times.

SYSTEM HEADEND INSTALLATION AND TESTING

Installation of the system headend is typically the first step of any implementation. The system headend for an ACS generally refers to the system servers and software as provided by the system manufacturer. In the past, the headend was typically composed of standalone servers that were dedicated to the operation of the ACS. Headends have evolved to include the use of virtualized servers that operate within a Virtualized Server Environment (VSE) and the use of cloud environments. However, headends can still include dedicated servers implemented in a traditional manner.

Regardless of server and software mechanism, the headend is the primary software that monitors the system, provides data to the monitoring and administrative workstations, and holds all of the transactional and programming data for the ACS. Due to the complex nature of the system implementation, sufficient time should be allocated to allow for the system headend to be tested prior to beginning the deployment of field equipment. This testing will demonstrate that the headend is stable and that there are no performance issues with the implementation. Depending upon the type and configuration of the system implemented, the headend installation will typically be fairly quick, often taking less than one week. However, testing for stability will typically take several weeks to allow for a thorough burn-in and to demonstrate system stability. For large systems, the burn-in may include factory acceptance testing prior to arriving at the site, or on-site if mandated by the airport.

SYSTEM INTEGRATION

The integration could include systems such as the VSS/CCTV system, the DAC service, IDMS, CBT, CAD, PSIM, and other systems as identified as part of the design.

Integration with ancillary systems should be established and tested as part of the system headend installation. Depending on the specific situation, this integration may be accomplished directly or may need to be configured in a test environment to provide proof of concept before being implemented into the production environment. The integrations should be fully tested before they are implemented. Existing systems that are to be integrated should also be tested to validate their functionality prior to the installation of the ACS field hardware.

DATABASE TRANSITION

Depending on the existing system configuration, it may be necessary to transition the database from the existing system to the new system. This transition would typically involve credentialing and cardholder data stored in the ACS. If the airport does not have an existing, separate IDMS and intends to continue with an ACS with integral credentialing, then the transition of that database will need to be planned and tested.

Some airports choose to re-enter the data instead of transitioning the data. This decision is typically based on the size of the facility, the overall condition of the data in the credentialing database, and whether old data has been removed from the system. If the time to clean up the data for the transition may exceed the time needed to re-enter the data, then the airport may choose a manual transition. This

may also be considered if the new system will have very specific data limitations and mechanisms that will bring the data into consistency. For example, if the employer field will be based on pull-down menus with predefined options, then the existing data may require extensive rework. The need to transition data should be considered in the Technical Design Phase so that the necessary resources are available in the Implementation and Integration Phase.

In addition to the credentialing database, the ACS will have configuration data that assigns access levels and/or portals to specific credential holders or credential types. The format of this data tends to vary depending on the ACS manufacturer, and the data is often not compatible between systems. Also, there may be dependencies within the system that need to be satisfied prior to allowing access to be assigned. First, the access points would need to be present in the system and programmed before being able to be assigned to a credential holder or access level, making the direct transfer impossible if the transition is phased. Second, specific access rights may be tied to credential features that have to be set within the credential type assignment. For example, many airport credentials have visible attributes that show that a person has rights to access airfield gates and drive within the AOA and Secured Area, and the credential will also include a Customs seal if the person has a CBP clearance. Many systems will not allow for access to specific areas, doors, or access levels unless the specific features are present on the credential. Whether this data can be transferred or will need to be manually set within the new system needs to be determined and accounted for as part of the transition.

If the airport has an existing, separate IDMS, then the integration of the IDMS will need to be planned but the transition of data between the legacy ACS and the new ACS should not be required. However, as the mechanisms for assigning doors and/or access levels often differ between systems as noted above, some reworking of the existing IDMS may be required and should be carefully planned.

Regardless of the transition strategy employed, the overall strategy should allow for access to the legacy system records. The retention of access records and credentialing data may be necessary after the last door is cut over from the system, and the existing system should be maintained until that time period expires. This period could exceed two years, depending on the longest assigned credential expiration duration and the required audit schedules. The ability to access data to remain in compliance and retrieve historical data needs to be carefully planned, and the maintenance of the existing system needs to accommodate that period.

PHASED IMPLEMENTATION

The order of phases is important to the success of the implementation. In some airports, the implementation of the ACS starts in a test lab environment, while others start at the airport in back-of-house spaces, or in a lightly used concourse or non-critical area. Either approach allows for issues to be discovered and rectified prior to moving into busier or more critical areas of the airport. Regardless of the approach, the phasing is vital as the cutover will often remove boarding doors and other critical portals from use for a period of time. Minimizing the impact to specific airline operations and coordinating the cutover is key to maintaining overall airport operation.

TRAINING

Training is an important part of system implementation and should include the personnel who interact with the ACS, such as system operators, system administrators, and others who will monitor or interact with the system headend. This training should be conducted both prior to the system going live and after implementation to allow for operators to address areas that were not clear during the initial training, or to address issues that may arise unexpectedly during the initial operation of the system.

Training should also be given to end users, including the system credential holders who will use card readers or biometrics, and who will be critical to the operational success of the ACS replacement. The training also can provide an opportunity to observe system usage and make adjustments to the system programming as necessary to minimize nuisance alarms.

PARALLEL SYSTEM OPERATION

Parallel system operation during any system implementation is expected. However, before commencing the transition to a new system, it is necessary to clearly define the expectations of how the parallel operation will be handled from an operational perspective, as well as how the existing system will be maintained, and how points will be removed as they are cutover to the new system.

While the overlap period will vary depending on the scope of the system implementation, the size of the facility, availability of funding, and other factors, it is important to consider the critical requirements for system monitoring, administration, and maintaining regulatory compliance during this overlap period. The overlap could range from several months to several years, and the operation of the systems during that overlap needs to be clearly defined. Depending on the configuration of the systems, the dual operation may require double entry of data, as well as monitoring of two distinct systems. This will result in an increased workload for system operators.

The parallel operation of two systems will also increase the load on the existing infrastructure such as the network, power systems including UPS, and the server environment, as well as increased processing on systems that may be integrated to both ACSs. This should be considered, and the conditions and capacities of the existing systems should be reviewed to ensure that they are adequately robust to support the parallel operation.

In some instances, it may be possible to temporarily integrate the legacy and new systems, removing the need to monitor two separate systems or double enter information and data. Facilities that use a separate primary user interface, such as an IDMS, PSIM, or CAD, may support a more seamless transition, allowing for it to occur over a longer period without interrupting the operation of the airport. In many such cases, the personnel monitoring the system are not aware of the transition, as it occurs in the background and is not evident to the operators. Regardless of the approach, the transition methodology and duration should be planned for and agreed to by all parties prior to the start of the implementation.

SYSTEM INSPECTION

System inspection should occur as each step of the Implementation and Integration Phase is completed, and should be performed by the appropriate airport ACS manager and the contractor. In addition to the ongoing inspections, a final verification and inspection should occur to ensure that all of the contracted work is complete, with each task verified or added as needed to direct the contractor to fulfill the contract requirements. While the final testing and commissioning may occur in parallel with the completion of this phase, both will need to be completed prior to system acceptance.

DISASTER RECOVERY AND CONTINGENCY PLAN

As part of the system implementation, it will be necessary to create a thorough Disaster Recovery and Contingency Plan. This plan will need to include items such as backup of the new and legacy ACSs, as well as address potential failures in the system. Disaster Recovery and Contingency Plans will likely vary based on the specific system proposed by the system contractor/integrator and the expected operation. Regardless, the costs for these plans need to be included, and any costs incurred due to a failure that is attributed to the contractor/integrator will be borne by the contractor/integrator as part of the project.

Table 5. Implementation and Integration Scope Checklist

Implementation and Integration Scope Checklist		
System Headend Installation and Testing	Install the system headend and test for proper operation and stability	
System Integration	Integrate ACS to other systems and test including:	
	• VSS/CCTV	
	• DAC	
	• CBT	
	• CAD	
	• PSIM	
	• Other system(s) identified as part of the design	
Database Transition	Determine if data will be transitioned or re-entered	
Phased Implementation	Phased implementation could include:	
	• Test lab environment	
	• Implementation in lightly used or back-of-house areas	
	• Implementation in site buildings and airfield/AOA gates	
	• Implementation in lower traffic areas of the airport	
	• Implementation in high traffic areas of the airport	
	• Implementation in high security areas such as CBP or other special use area	
Training	Training should include:	
	• Training for system operators	
	• Training for system administrators	
	• Training for credential holders for revised field hardware	
	Training should occur:	
	• Prior to start of system implementation	
	• Post-implementation training	
Parallel System Operation	For most system transitions, dual system operation will be necessary. The operation and monitoring of the two systems needs to be planned. The process may include:	
	• Monitoring two systems concurrently	
	• Integration of the new and legacy ACS to allow monitoring of all alarms in a single system	
	• Integration to a PSIM, IDMS, or CAD system, with those systems acting as the monitoring interface	
Airport Security during Transition	Additional security requirements during installation and construction: including:	

Implementation and Integration Scope Checklist		
	• Guard services	
	• Additional security monitoring personnel during transition	
	• Overtime or additional full-time equivalent employee to support installation	
	• Other additional personnel needs	
System Inspection	System inspection will include:	
	• Inspection and verification of proper installation of all system equipment at all portals and other ACS points	
	• Inspection and verification of proper installation of conduit and cabling from the ACS portal or point to the communication room	
	• Inspection and verification of the ACS field panels and power supplies	
Disaster Recovery and Contingency Plan	Disaster Recovery and Contingency Plan should include:	
	• Backup of new and legacy systems	
	• Address possible system failures	

4.6 Phase 6: Preparing for Operations and Maintenance

Phase 6, Preparing for Operations and Maintenance occurs after the transition to a new or upgraded ACS has been completed, but there are several aspects of this phase that should be considered during the ACS Transition Process. Phase 6 focuses on finalizing system documentation and developing critical operations and maintenance plans to ensure that the system is optimized over the life cycle and remains at full operational capability. The Preparing for Operations and Maintenance phase always establishes a solid foundation for future decision-making on ACS operations.

This phase seeks to answer the following questions:

- Have detailed as-builts been provided, and is there a schedule for routine updates to the documentation?
- Have inspections been conducted to confirm full operational capability of the system in accordance with defined requirements?
- What will the strategy be for ongoing maintenance and support for the ACS? Will it be performed in-house, by outside contractors, or by some combination of the two?
- If maintenance will be performed in-house, have all maintainers and system administrators been adequately trained?
- What service levels does the ACS require to be effective, and how should these be enforced?

Outcome: Documented system features, infrastructure diagrams, and information that results in ease of decision-making regarding future ACS modifications and add-ons.

Once the system implementation is complete, the closeout of the project needs to be completed to allow for the system to transition from an active construction project to the Operations and Maintenance phase. The following are the steps that should be considered during this time:

SYSTEM ACCEPTANCE TESTING AND COMMISSIONING

System testing and commissioning is required to validate proper operation. This will include active monitoring of the system for errors that may indicate improper installation or programming. For example, line errors may show an issue with the installation of resistors used to monitor the system, or could indicate an incorrect program setting in the ACS. Additionally, a preponderance of alarms on a specific door could indicate an issue with the installation of devices at that door. By running reports on the system during this phase, the contractor can identify the issues and resolve them directly. Issues can be recorded by the system operators, or the contractor can be asked to monitor the system and proactively resolve any issues that arise.

Any system-generated reports required for inspections and audits will also need to be created and validated at this time to ensure they include all necessary data points, as identified in the Technical Design phase.

System testing and commissioning can include multiple levels of testing, from a phased approach to an overall system test. During this step, airports may verify correct operation of the system and require a System Availability Test to demonstrate system stability. The exact testing and commissioning regimen should be clearly defined in the specifications to ensure that all of the required tests are performed.

SYSTEM SUPPORT AND MAINTENANCE

The strategies used by airports for system support and maintenance vary quite widely across the industry. Some airports elect to outsource the support and maintenance to the contractor/integrator, with full support provided as part of the outsourcing agreement. A decision such as this is typically based on the business model of the specific airport, but is not necessarily related to the size of the airport. Some large airports have the contractor/integrator provide full support on a 24/7 basis, including a Service Level Agreement to ensure the proper response. Other large airports may provide the first response from airport personnel, with the contractor/integrator providing higher tier support that requires escalation. Much of the decision for these airports is based on the staffing levels and the structure of the organization.

Smaller airports also tend to have a mix of strategies, with some small airports relying on a fully outsourced response due to limited staffing availability and others providing varying levels of support. For support and maintenance, there is not a single one-size-fits-all approach; the pros and cons of each approach will need to be weighed against the ongoing costs of contracting with the contractor/integrator and the response metrics required by the airport. In addition, considerations such as whether the ACS is applied to a single facility or multiple facilities, if the staff at the airport is unionized, or if the systems are under the purview of a city, county, or state agency may also impact the decision.

SYSTEM SUPPORT AND MAINTENANCE BY CONTRACTOR/INTEGRATOR

As noted in Section 4.4, Procurement and Solicitation, warranties, available extended warranties, costs for software and hardware version upgrades and bug fixes, availability of future features, ongoing licensing and manufacturer support costs, and short- and long-term maintenance requirements and agreements are often included as part of the system procurement, with the contractor receiving a three- to five-year contract to support operation and maintenance of the system. This approach can result in the contractor/integrator becoming an integral long-term team member of the airport.

ALTERNATE SYSTEM SUPPORT AND MAINTENANCE

Some airports choose to use internal staff for operational maintenance and support. In such cases, the airport will typically have multiple personnel that have been trained and certified on the ACS. While an integrator is available in most of these types of arrangements, they are used primarily to supply parts and

for additional support as needed. As many manufacturers do not sell parts or provide support directly to customers, an integrator may still be required, and a fee will likely be associated with having this entity act in this role. In rare cases, the manufacturer will contract directly with the airport.

An airport's decision to self-support maintenance functions should be based on having adequate, properly trained/certified staff with minimal turnover and demonstrated longevity. If personnel tend to transfer between groups or to not stay at the airport long term, this type of arrangement may not be viable. Many component and system suppliers/manufacturers require that warranty, service, and maintenance be performed by authorized or certified representatives, dealers, or distributors. Any consideration of alternate support must include review of such requirements.

SYSTEM AS-BUILTS

As the project is completed, contract specifications should include the creation of as-built documentation for the system, including any and all Operations and Maintenance Manuals and system documentation.

The integrator will typically provide as-built drawings for the system, mostly based on the original design drawings as well as the shop drawings produced as part of the implementation. As system expansions and modifications occur, the integrator will need to update system documentation to reflect the revisions. Ensuring that system documentation is current and maintained is critical for effectively managing the system as it matures. The creation of system as-builts should be included as part of the System Maintenance contract.

All airports agreed that ensuring system documentation and as-builts were provided was critical, and that the airport should ensure that these are delivered by the contractor/integrator before project completion. The as-builts and documentation should be reviewed before acceptance by the airport, and they should be kept up to date to account for all moves/additions/changes to the system over time.

UPDATE DISASTER RECOVERY AND CONTINGENCY PLAN

Once the implementation phase is complete and the system is accepted by the airport, the Disaster Recovery and Contingency Plans will need to be updated. If the contractor/integrator is to provide system maintenance, then portions of the overall strategy may remain the same. Conversely, the airport may wish to take a more active role in the Disaster Recovery and Contingency planning, with airport personnel providing backup and other routine functions. Depending on the system implementation, such as the use of virtualization, or centralized or cloud storage, it may make more sense for the airport to manage those aspects, especially if the servers or storage are shared with non-security airport systems.

Table 6. Operations and Maintenance Scope Checklist

Operations and Maintenance Scope Checklist		
System Testing and Commissioning	Validation of the system installation and operation will include:	
	• System testing to prove proper operation of all system devices and equipment	
	• System commissioning to validate the proper operation of the overall system	
System Support and Maintenance	Ongoing maintenance will be required. Maintenance may include:	
	• Maintenance by the system integrator as a follow-on activity from the installation, overseen by the airport	

	• Maintenance by a third-party certified provider for the system, overseen by the airport	
	• Maintenance by a combination of integrator or third-party provider plus trained and certified personnel at the airport	
	• Primary maintenance and support by the airport, with an integrator or third-party vendor providing support as needed	
System As-Builts	System as-builts need to be received, reviewed, and verified at the completion of construction	
	Integrator will need to keep them up-to-date as part of the ongoing maintenance of the system	
	As-built updates including all move/add/changes should be part of the ongoing maintenance contract	
Update Disaster Recovery and Contingency Plan	Update parts of the plan that changed during Implementation and Integration	
	Airport personnel may take an active role in managing routine aspects or components that share equipment with other airport systems	

4.7 Future Planning

Future Planning starts at the Project Scoping and Planning phase and runs through each of the subsequent phases. Thoughtful planning and decision-making that consider future needs can help streamline future ACS upgrades and system transitions. Active monitoring of security, regulatory, and technology trends, along with detailed documentation of user groups and decisions, can help inform future efforts and avoid challenges that may have been experienced during the initial transition.

Future planning seeks to answer the following questions:

- Has a method been developed to document decision-making and user community inputs to help inform future ACS planning efforts?
- Is there an adequate understanding of potential future security and regulatory landscapes to help ensure the ACS is capable of meeting updated requirements?
- What technologies are envisioned for use in the next 5–10 years that may impact the ACS?
- What measures have been taken to address ACS scalability and expansion in the future?

Outcome: Implementation of a flexible ACS that can grow with changing operational and regulatory landscapes.

Future planning can be informed by the following:

ONGOING SYSTEM COSTS

While the majority of costs for an ACS are incurred during the system installation, airports should consider recurring or future-related costs. These can include warranties, software licensing costs, software and hardware version upgrades and bug fixes, future features, short- and long-term maintenance requirements, and contracts for integrator support. These need to be considered and budgeted for to ensure that they are adequately funded after system installation.

SYSTEM EXPANSION

System scalability to support future expansion is an important consideration. The selected ACS's expansion capabilities should be clearly defined as part of the design so that it is not necessary to

upgrade to another software version to achieve the original objectives. Ensuring that the system is designed to accommodate any expected expansion can result in cost-savings in the future.

The system should be planned to be upgradable by adding licensing and field panels as required, with no significant work to the system headend beyond programming. All systems should have significant expansion capability without requiring server replacements or major system upgrades.

ENHANCEMENT OPTIONS

The ACS RFP and design should ensure that future enhancements and features can be implemented.

FUTURE TECHNOLOGY INTEGRATION

A key consideration is ensuring that future technologies can be integrated with the ACS without requiring significant upgrades. Having a roadmap of the desired features, and working with the system manufacturers to vet the desired features against the manufacturer roadmap, should be included as a part of the procurement process.

POTENTIAL REGULATORY CHANGES

Regulatory changes are expected. Most of the major manufacturers in the marketplace are aware of the expected changes that are being discussed and have a roadmap to accommodate those changes. One of the most important lessons learned from this research is that an airport should consider a potential vendor's experience and number of installations in the airport market as part of any procurement, as this will show the dedication to adapt to any regulatory requirements.

Table 7. Future Planning Scope Checklist

Future Planning Scope Checklist		
Ongoing System Costs	Ongoing system costs may include:	
	• Ongoing integrator service agreement costs	
	• Software maintenance and support costs (SSA)	
	• Ongoing licensing fees	
	• Integration maintenance costs	
System Expansion	The ACS should have the ability to expand, including:	
	• Ability to add readers and devices without major upgrades	
	• Ability to support expansion, additions, and added features without requiring headend upgrades or replacement	
Enhancement Options	The ACS should be able to implement new enhancements and features	
Future Technology Integration	The ACS should have the ability to:	
	• Incorporate future technologies that were identified in the Market Survey	
	• Have a roadmap to include desired features identified as future enhancements	
Potential Regulatory Changes	The ACS should be able to adapt to regulatory changes	
	• Manufacturer may have a roadmap of anticipated regulatory changes	

SECTION 5: EVOLUTION OF ACS TECHNOLOGY, KEY TRENDS, AND CONSIDERATIONS

In recent years, system developers have rapidly innovated ACS technologies, resulting in more complex and capable systems. ACS technologies consist of many components that include readers and other equipment on portals, reader interface panels, and system controllers that communicate across networks to headend servers. Each component in the chain serves a specific function in the operation of an ACS. While this research focused largely on immediate transition needs, it is important that airport operators consider new and emerging trends in technologies, and how those future capabilities may impact current replacement and upgrade decision-making.

- **Credential Readers –** Credential readers serve as the primary user interface to an ACS. The primary function of a reader is to allow for a person to present their credential for system verification to initiate the opening of an access control point, such as a SIDA door or a baggage chop door.[12]
- **Biometrics –** Biometrics have evolved from the early implementations, using single fingerprint or hand geometry, to include other biometrics such as iris or retinal scan, vascular recognition, contactless fingerprint, and facial recognition.
- **System Infrastructure and Communication Protocols –** ACS technologies have evolved from serial communication to IP-based systems, although many still have elements of serial communication and other low-security communication protocols. Most ACSs have transitioned from dedicated infrastructure to encrypted communication over the LAN, but the communication to the readers is often still a low-security protocol such as Wiegand. However, the industry has started to move towards encrypted communication end-to-end using Open Supervised Device Protocol (OSDP) and similar communication. To provide a fully secured system, the overall system infrastructure will need to move towards leveraging the airport's IT infrastructure and securing the remaining elements.
- **Servers –** ACS servers have traditionally been dedicated, standalone physical servers, but the recent trends have been toward the use of virtualized servers within the facilities' VSE or to a cloud-based server.

5.1 Credential Readers and Credentials

Credential readers and the associated credentials have evolved since these were first installed in airports decades ago. Many of the earliest applications were magnetic stripe technology. Magnetic stripe has several limitations. First, this is a contact technology, requiring that the read heads come into contact with the magnetic stripe. This leads to wear on the read heads as well as on the magnetic stripes on the cards, which results in failures with both cards and readers, requiring maintenance of the readers, especially the outdoor readers. In addition, magnetic stripe is not secure and can be duplicated relatively easily, as has been evidenced by skimmer technology placed at pay locations such as ATMs. Due to these limitations, the industry began moving toward contactless technology in the late 1990s.

PROXIMITY CARDS AND READERS

The first contactless technology was the proximity reader, which used a card that was pre-encoded and operated at 125kHz. The card had a good read range and, when it first became available, it was

[12] For an in-depth analysis of considerations related to access credential technology, please refer to PARAS 0017 *Access Control Card Technology Guidance*.

considered secure as it was not a common media type. However, as the media grew in popularity, it became common for duplicate card numbers to be issued, and users were finding that their parking garage card could also be used on the airport ACS. To reduce the possible overlap of card numbers, the site code was added to the card, allowing for a two-factor authentication of the card data, requiring the correct site code and card number. Though this did reduce the overlap, the proximity card is still not encoded, and has become fairly easy to replicate. For example, kiosks in some home improvement stores can be used to duplicate these cards.

Another security measure that is fairly common is to add factors of authentication to the process of gaining access through an ACS portal. The most common authentication is to associate a Personal Identification Number (PIN) to the card, requiring that a valid card read occur plus a PIN to be entered on the reader that corresponds with that card. The PIN is stored only in the ACS headend, which prevents a copied, stolen, or found card from being used at a portal. The use of a PIN is considered the first authentication level. However, the PIN is not a completely secure authentication means. For example, an authorized person can simply disclose the PIN to an unauthorized person, or an unauthorized person can observe a person entering their PIN on the reader. While additional layers of authentication do remove some of the vulnerability associated with both magnetic stripe and proximity cards, these card types are still limited and the technology used by the industry has evolved.

CONTACTLESS SMART CARDS AND READERS

Contactless smart cards operate at 13.46 MHz and typically include an unencrypted area as well as an encrypted area. The encrypted area is available in different memory sizes dependent upon the type of information that will be stored on the card. The first generation of readers and cards used a Data Encryption Standard (DES) encryption; however, this was compromised and is now considered non-secure. More recent generations have moved to an Advanced Encryption Standard (AES) encryption.

The use of current generation contactless smart cards and readers with the latest encryption is recommended as part of any ACS upgrade to enhance the integrity of the access media.

OTHER CARD AND READER TECHNOLOGIES

Other reader technologies include contact type cards, which are often associated with National Institute of Standards and Technology related applications. These are not typical of airports. However, some airports have specified readers that provide this capability or higher security contactless card capability such as Personal Identity Verification, Transportation Worker Identification Card, or First Responder Authentication Credential compatibility to meet user needs in the facility, such as TSA or CBP.

Another technology that has come into the marketplace is Bluetooth-enabled readers. Many system manufacturers have a smart phone app that allows for the phone to be used as a credential at an enabled reader, with the system reporting the same card number for access either by the card or the Bluetooth credential. While readers with this technology may not be used in situations requiring regulatory compliance, or where the airport-issued identification credential needs to be verified prior to entering the SIDA, it could be considered for non-regulated areas such as parking entry or office spaces. One of the advantages of Bluetooth is the increased range over the smart card technology. It may allow, for instance, for users to access a parking lot without needing to roll down the windows of their car.

In addition, some manufacturers have begun offering features such as the Secure Identity Object (SIO) to further enhance encryption. Features such as these may not be compatible with all ACS manufacturers' products, so specifying some additional proprietary features could limit the available system manufacturers. It is expected that encryption schemes will continue to evolve, and that the manufacturers will continue to enhance security features and capabilities. The card and reader

technologies in the marketplace will need to be evaluated as part of the project design to ensure that the latest encryption technology is specified.

MULTI-TECHNOLOGY CARDS AND READERS

In order to facilitate and support the ACS Transition Process, the industry offers multi-technology cards and readers. For example, if a facility is currently operating on a proximity card, implementing a multiclass reader would allow for the existing cards to be read by the newer readers during the card technology transition, making the switchover seamless to the system end users. As the transition to a new card media could take up to two years depending upon the expiration period used by the airport, the use of multiclass type readers and cards can be invaluable. Once the legacy card stock is fully removed from the card population, then the legacy format can be shut off to make the readers only capable of reading the newer technology cards.

READER COMMUNICATION STANDARDS

In addition to card-to-reader security, the connection between the card reader and Access Control Interface Board should be considered. The traditional means to communicate with card readers has been RS-485 and Wiegand, with Wiegand being the most common protocol in use for reader communication. However, Wiegand has characteristics that impact its capabilities and security:

- Wiegand has a fairly short transmission distance and is also susceptible to interference, requiring shielded cable to ensure data integrity. Even using these measures, many airports have experienced issues when installing readers on passenger boarding bridges, in elevators, and in areas with high voltage or other sources of electromagnetic interference.
- Wiegand is a unidirectional communication means, so communication to the edge devices[13] has not been possible. Therefore, any programming changes to card readers or firmware updates have required accessing the reader directly, which can be a time-consuming process.
- Wiegand is a non-encrypted communication method. This means that any data sent from the reader to the Access Control Interface Board can be intercepted and possibly used to spoof the ACS in a man-in-the-middle type of attack. The main means used to prevent this type of attack had been physical protection of the card reader cabling by installing the cabling in conduit, providing tamper switches at the reader and at interconnection boxes, and use of high security screws. However, should the cabling be accessed, the data captured can be used to spoof not only a card read but also any additional authentication data that is sent to the system headend.

To overcome many of these issues, the industry has developed the OSDP standard. OSDP is a fully encrypted, bi-directional communication protocol that is based on the RS-485 communication that provides higher security and a longer transmission distance capability than traditional Wiegand. Overall, this protocol overcomes most of the limitations that were noted in regard to Wiegand. It is recommended that any readers implemented be provided with OSDP capability, and the OSDP capability should be used where possible.

5.2 Biometrics

Biometrics in airports have been predominantly hand- and finger-based, contact-type biometrics. While other biometrics such as retina and iris have been used, these have not had the same level of acceptance

[13] In this context, “edge device” is a single ACS hardware component that provides an entry point and/or an interface to the ACS as a whole (e.g., an access card reader).

in the marketplace as hand/finger-based biometrics. However, in recent years, newer generations of biometrics integrated with the card reader have begun to make inroads in the airport environment.

The first newer generation of biometric was a contactless fingerprint-based biometric. This biometric allowed for a user to pass their fingers through a slot in the reader, and the unit would read all of the fingerprints presented, allowing for authentication to be based upon a single finger or multiple fingers. As this is contactless, it is not necessary to place the finger in a specific location on a sensor, making the technology more user-friendly and a faster method for verification.

The second contactless biometric technology to become more common in the marketplace is facial recognition. This technology uses an image of a person's face to authenticate the identity of the person. This type of biometric is being used by CBP for verification of passengers for the Global Entry program. Combination card readers with integral facial recognition capability have been introduced, allowing for more seamless operation with ACSs.

In addition to these technologies, iris-based biometrics continue to be available in the marketplace. Iris biometrics have traditionally been mostly contactless, but some units required the sensor to be adjusted to view the iris. Newer units do not require the user to adjust the sensor, making the technology more user-friendly and requiring less contact, making it similar to the contactless fingerprint and facial recognition devices.

Other biometrics available as part of separate systems include voice recognition, gait recognition, bio-based data from fitness tracking type devices, and video analytic-based facial recognition systems. These technologies have not yet been brought to market in an integrated unit with a card reader, and would typically be separate systems that would need to be integrated with an ACS. Regardless of the technology and biometric, the main factors that should be considered are the false rejection rate, the false acceptance rate, ease of use, and user perception of the intrusiveness of the biometric.

Another factor airports must consider is the manner in which identification is made in conjunction with the ACS. There are two methods that are typically used: a one-to-many comparison and a one-to-one comparison. In the one-to-many comparison, the biometric is analyzed by the biometric reader and then compared against a database of enrolled users. The system selects the match and waits for the ACS to match the user-presented credential to the identified biometric. The ACS reader will read the encrypted card number and send the number to the ACS headend, which will verify whether the card is valid and provides appropriate access rights. If the card and access rights are valid, and the biometric and credential match, the ACS will grant access.

In a one-to-one comparison, the user presents their card to the reader, which either reads a biometric template and card number that are stored on the card, or reads the card number to locate a corresponding template in the system database. The reader will then request that the user provide the biometric and will compare the presented biometric to the template. If the biometric and template match, the card reader will then send the card number to the ACS for card validation and confirmation of access privileges, and then the ACS will grant access.

While each authentication mode has pros and cons, as the user population grows, the one-to-one comparison tends to have more advantages as it is faster and provides a higher level of accuracy. However, some users have expressed concern with biometric templates being stored in the cards, even if encrypted. The biometric template is typically a mathematical interpretation of a person's face or fingerprint, meaning that most systems do not store an actual image on the card, thereby reducing privacy concerns. Also, encoding the template into the card and having the comparison occur at the

reader level is a much easier integration than using a headend integration between a biometric system and the ACS, so this should also be considered.

5.3 System Infrastructure and Communication Protocols

Early ACSs started with serial communication from the headend to the field panels, but that was quickly supplanted by network connectivity. As networking technology has progressed, so has the networking for the ACS field panels. Nearly all of the system controllers use standard IP LAN connections to communicate with the ACS headend, increasing the speed of the connection and improving encryption and security. The current market offers traditional architecture, with a primary intelligent system controller that interfaces with the LAN and then communicates with the reader boards using serial connections, although these connections now offer encryption such as OSDP. Some manufacturers offer boards that are LAN connected and forego the serial connections altogether, with some offering levels of intelligence within all boards and others offering boards that act as slave units to the main controller board.

When deciding between LAN and serial connections for system communications, airports should consider exactly how the system will be designed and how many LAN switch ports may be needed to support the system. Overall, the reliability of the different architectures is comparable, as is the level of security. All of the different system configurations offer pros and cons, and the use of each should be considered in regard to the expected location of the boards. If the airport prefers to consolidate the boards in the communication rooms, then the use of an IP-connected controller that uses a serial connection to the reader boards may be appropriate. If the boards will be distributed to locations at each access control point, then the use of individual IP-connected boards at each access control point may be appropriate.

As part of the overall design, the infrastructure to support power and other considerations, such as fire alarm release, may need to be considered. For example, if individual IP boards are placed at doors, the boards can often use PoE for power. However, if the door hardware and associated devices have a draw that exceeds the PoE capacity, then additional power supplies or cabling from the communication rooms would be required to provide power, which would reduce the viability of this approach.

In addition, the serviceability of the components and the architectural and aesthetic impact need to be considered. With many airports having open ceilings and large expanses of glass, placing a controller board above a portal may not be possible, or the controller may end up being at a height or location that would prevent being serviced while the general public is present.

As newer encryption types and security features are added to the marketplace, it is reasonable to expect that ACS manufacturers will continue to adopt the latest security features in their systems. For airports, these security features should be a prime consideration when procuring an ACS. While ACSs have often been relegated to a segregated, isolated LAN with standalone server, it is expected that modern ACSs can be implemented in the VSE using the same storage solutions that airports employ to support typical operations. By moving into mainstream technologies, the cost of implementing and operating the ACS will be much lower.

5.4 Servers

The traditional ACS would be implemented using physical servers—typically a minimum of two—in separate locations to provide a redundant capability. With the advent of virtualization and cloud computing, architecture has changed and offers a wider variety of implementation options. The use of

virtualized servers become more common at airports for their overall operational needs. The implementation of the ACS headend as part of a VSE is becoming commonplace and offers many advantages:

- The use of a VSE can provide additional levels of redundancy, with the redundant server often being able to be brought online instantaneously upon the detection of a fault or issue with the main server. This allows for a very rapid recovery in the event of a failure.
- Without the need for dedicated equipment, the server resources can be adjusted to fit the needs of the system, enabling users to easily add resources to the configuration on the fly and without requiring the replacement of hardware.
- The use of the VSE allows for the ACS servers and environment to be managed as part of the overall airport environment, removing the need for dedicated resources to oversee the ACS server environment and manage the hardware upgrades. While the use of a VSE can provide additional capabilities, the individual ACS products should be evaluated to determine what features and capabilities are available and can be fully utilized within the VSE. Not all systems may be able to take advantage of these capabilities, and this will need to be understood as part of the ACS procurement if a VSE is a priority for the airport.

In addition to the VSE, another trend is to use cloud resources for the servers. Many different companies offer cloud computing capabilities that include hosting servers and storage, with those entities managing the hardware and the virtualized environment. The use of a cloud resource, especially for a smaller facility that may not have redundant data centers, could address a requirement to provide a level of redundancy that may not be readily available at the airport. While this is a viable option, considerations in regard to security of the system and the associated data, the reliability and redundancy of the internet connection at the airport, and the costs associated with hosting will need to be carefully evaluated. If redundant internet connections are not available or if the reliability of the connections is not optimal, then the use of a cloud resource as the sole headend would not be recommended. Most airports that are considering the use of cloud resources plan to use them for backup purposes and/or to support remote facilities for entities that may operate at multiple airports.

This type of configuration will continue to expand, and may eventually become the predominant system architecture. However, the full impact and applicable security concerns of cloud resources should be considered before implementing this type of solution.

5.5 Door Hardware

Door hardware has evolved significantly in the past decade and offers many more options than the traditional lock hardware. Locking means at airports have typically been a mix of electric strikes, magnetic locks, and electrified door hardware components. The current direction of the industry is to use door hardware-centric type of equipment, which includes electrified mortise locks, electrified panic hardware, and other types of electrified hardware.

When selecting hardware, the first consideration raised is often the appearance of the hardware. The style and finish of the visible hardware is an important consideration for the aesthetic of the airport. But, as most hardware types are available in a wide variety of finishes and styles, this concern may be addressed after the other factors are considered.

Electrified door hardware mechanisms have become a much more popular and mainstream option for controlling doors. Several Cat X airports and numerous smaller airports have implemented the solutions described below. The implementation of door hardware-based control equipment has demonstrated the

durability of the equipment and its ability to withstand the rigors of the airport environment. However, in order for a door hardware-based solution to be effective, the doors must be in good repair and operate smoothly. If the doors do not align well, do not close fully, or otherwise require modification to accommodate the door hardware, then the airport will have to consider the continued use of other hardware or consider replacing or upgrading the doors as part of the ACS replacement. As door replacement can add significant costs to the project, this factor should be considered as part of the project scoping and budgeting.

FAIL SAFE VS. FAIL SECURE

From an ACS perspective, the first consideration for door hardware is whether the door is a fire egress door. If so, it will be necessary to determine the proper hardware type. The occupancy will determine if panic hardware is needed, or if traditional door handsets are allowable. The specific life safety code in use at the airport will specify whether the use of delayed egress is allowed. Depending upon the direction of egress, the access control point may need to be released upon a fire alarm. For example, if a door is controlling access in the direction of egress, then that door will need to be connected to the fire alarm so that it can be released upon a fire alarm in that zone. This means that the door will provide a fail safe condition in the event of a power failure or a fire alarm. A fail safe device or mode means that in the case of emergency the door will be unlocked to allow egress.

If a door is not required for egress or to allow access in the case of a power failure or a fire alarm, then the door is referred to as fail secure. Fundamentally, fail safe door hardware requires power to keep the door hardware locked, while fail secure door hardware requires power to unlock the door hardware. This means that power consumption for fail safe door hardware will be a nearly continuous load, while fail secure hardware will represent an infrequent load on the system.

The approach to determining what doors will be fail safe or fail secure should be based on the required egress, the sensitivity of the area, and the need to provide protection for the area in question. Fail safe door hardware is intrinsically more vulnerable to unauthorized entry by disconnecting or otherwise interrupting the power to the lock.

ELECTRIFIED MORTISE LOCKS

The electrified mortise lock is becoming one of the more popular locking means for access-controlled doors. These locks have many good features and capabilities. First, the electrified mortise can fit into any door that is designed to accept a mortise lock, requiring only minor modifications. For hollow metal doors, the electrified mortise should be a direct replacement, the routing of power should be straight forward, and power transfer equipment can be added with relative ease. The electrified mortise is available with one lever controlled and the other free to use or with both levers controlled. The units can be either fail safe or fail secure; the function for many manufacturers can be field selectable by changing a switch or jumper on the lock case, and the handing and latch bolt can be reversed in the field. The units typically have very low power draw.

Electrified mortise locks are available with REX function, latch bolt monitor, deadbolt monitor (if equipped), and a door position sensor. With the available features, the status of the lock can be monitored by the ACS, and is nearly invisible and seamless to the system users.

ELECTRIFIED PANIC HARDWARE

Some doors may require the use of panic hardware to comply with fire/life safety requirements. Some panic hardware interfaces with an electric mortise lock, while others use different locking mechanisms, such as electrified panic hardware that uses rim latch bolts or internal rods.

The use of an electric latch retraction can be considered. The older latch retraction units used a solenoid to retract the latch, which drew significant power and was loud during operation. The newer latch retraction units draw much less power and are nearly silent. As a side benefit, the unit will physically pull in the panic bar, indicating to the user that access has been granted, and allowing for the door to be accessed without depressing the panic bar. In addition to the electric latch retraction, the panic hardware can also be equipped with REX and latch bolt monitoring, providing additional monitoring features and functionality.

If allowed by the life safety codes in use at the airport, electrified panic hardware with delayed egress functions can be used. However, the options for these units are more restricted; features such as electric latch retraction and integral REX on the non-egress side of the door are not widely available. Delayed egress locks will always be fail safe in accordance with applicable fire and life safety codes.

ALL-IN-ONE DOOR HARDWARE

All-in-one type locks are available in the marketplace. These locks typically include card readers, and can also be equipped with PIN pads, monitoring of the lock status, and often a door position switch. These units will typically replace the existing door handle, and are only for doors that would be card/PIN entry and REX. They are available with internal memory or as online units that operate as any other access control access point, with card reads being validated by the ACS.

These types of locks are typically installed as wired units, with a network drop provided to the lock that also provides the power via PoE. However, there are other options available that operate on battery and communicate wirelessly, either over a dedicated wireless network or a facility's Wi-Fi network. The use of wireless locks is sometimes viewed as a possible security issue, as they could present a security vulnerability to the ACS headend through the wireless network. Wireless networks can be interrupted or jammed, preventing the updating of data or the sending of access or alarm events. Also, wireless locks are typically battery-operated, which can be a maintenance issue if the door is frequently accessed. Generally, the wired units would be more appropriate if the door has an associated regulatory requirement, but either can be considered. Overall, the cost of implementing an all-in-one unit is much lower than a traditional ACS portal, which can be a significant consideration for airports with limited funding.

5.6 Intelligent Power Supplies

As the Internet of Things has evolved, many types of systems that did not traditionally provide data analytics have been redesigned to enable system monitoring and data analytic capability for alarms and service notifications for equipment. One such system is the power supplies used for ACS. Intelligent power supplies provide notifications in the event of a power supply failure, enable monitoring of the individual power outputs and notify if a fuse or breaker is tripped or if the power draw falls outside of the programmed limit, and provide testing results for battery backup and other features. These types of features can alert maintenance personnel to a possible issue with a device, sometimes prior to the device actually failing. This allows for the equipment to be serviced prior to the portal becoming inoperable, or to address systems that go out of service before users are aware of the failure. Intelligent power supplies can also record the power usage of the system and possibly save resources by allowing for a more realistic sizing of battery backup and UPS units while maintaining the target durations.

The status of an entry point upon loss of power is determined by whether the physical barrier is fail safe or fail secure, which impacts the power draw. After meeting all life safety and AHJ requirements, the choice of mode will be closely related to the security objectives of the airport and the availability of emergency power through UPS or other backup electrical power (such as a generator).

SECTION 6: LEGAL IMPLICATIONS AND DATA PROTECTION CONSIDERATIONS

This section discusses the need to protect data and, in particular, airport employee PII, and the practical implications of these requirements on an airport ACS transition. Airports are encouraged to review PARAS 0007 *Quick Guide for Airport Cybersecurity*[14] for detailed information regarding cybersecurity considerations specific to the airport environment.

> General information is provided on these topics based on the literature review and learnings from interviews with airports and subject matter experts. This information is not legal advice. Airports and others with specific concerns regarding these matters should seek assistance from qualified legal counsel.

6.1 Protection of PII

PII has been defined by US government agencies as including:

> "(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date, and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[15]

Examples of PII include but are not limited to:

- **Name:** full name, maiden name, mother's maiden name, and aliases
- **Personal identification numbers:** social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, financial account numbers, and credit card numbers
- **Personal address information:** street address and email address
- **Personal telephone numbers**
- **Personal characteristics:** photographs (particularly of face or other identifying characteristics), fingerprints, and handwriting
- **Biometric data:** retina scans, voice signatures, and facial geometry
- **Information identifying personally owned property:** VIN numbers and title numbers
- **Asset information:** IP and Media Access Control (MAC) addresses that consistently link to a particular person

In some ACS configurations, data collection may include the collection of PII from badged personnel. Some examples of potential scenarios involving PII and an airport ACS include:

- **Vetting and credentialing.** PII collected by the airport during the credentialing and vetting process may be stored in the airport ACS or IDMS. This may include employee photographs.

[14] National Sake Skies Alliance, *Quick Guide for Airport Cybersecurity*, https://www.sskies.org/images/uploads/subpage/PARAS_0007.CybersecurityQuickGuide.FinalReport.pdf.
[15] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf.

- **Biometric-enabled ACS technology.** A biometric-enabled ACS may collect and verify employee iris, facial, or fingerprint data against a database of this information each time an employee enters the secure area of an airport.

> **Best Practice:** Airports should consider storing minutiae rather than the full biometric. Fingerprint minutiae are encrypted, secure, discrete data points used by most fingerprint recognition systems.

Regardless of how it is collected, protection of PII is an important issue. Several of the airport ACS subject matter experts interviewed stated that cybersecurity protection of data is a significant and growing challenge facing all airports. This is a particular concern for airport ACS because the ACS may be used by thousands of individuals.

While the research did not reveal any data breaches involving airport ACSs, there have been publicly reported cyberattacks involving airport employee data from other sources.[16]

> **Best Practice:** During the Project Scoping and Planning phase of the ACS Transition Process, airport managers should identify where, when, and how airport employee PII is collected and stored, as well as the specific types of data being collected.

There are security, business, and legal implications associated with the protection of PII. The security implications are critical. If employee PII is not protected adequately, it could be used by bad actors to compromise airport security and safety, such as by creating counterfeit identification materials, or by helping bad actors impersonate vetted employees to gain access to secure locations or important airport IT systems.

Business implications are also an important consideration. An airport's stakeholders expect an airport to safeguard PII that is provided to the airport during the normal course of business. There could be serious reputational and economic damage incurred as a result of not adequately protecting the PII of stakeholders that also use the airport ACS. A data breach of employee PII could negatively impact morale, productivity, and worker retention.

There are also direct costs associated with responding to and remediating a data breach. These costs have been significant for businesses in general. A recent survey conducted by IBM estimated that the average cost of a data breach to a US organization or business was approximately $8.6 million.[17]

6.2 US Federal Regulatory Environment

In addition to these security and business concerns, airports undertaking an ACS transition need to consider the legal implications and requirements associated with protecting airport employee biometric and PII data. The US legal and regulatory environment surrounding data protection, data privacy, biometrics, and PII is evolving rapidly. While no central data privacy or data protection law has yet been enacted at the US federal level, there are several narrowly focused laws with data privacy requirements, including the Health Insurance Portability and Accountability Act (HIPAA), which has extensive

[16] Davey Winder, "San Francisco Airport Cyber Attack Confirmed: Windows Passwords Stolen," *Forbes*, April 11, 2020, https://www.forbes.com/sites/daveywinder/2020/04/11/san-francisco-airport-cyber-attack-confirmed-windows-passwords-stolen/?sh=678a6f825b9c.
[17] IBM Security, *Cost of a Data Breach Report 2020*, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.

regulations regarding the collection and protection of health-related PII, and the Gramm-Leach-Bliley Act (GLBA), which restricts how individuals' financial data can be shared. While these laws are only tangentially related to airport employee PII, airport managers may wish to confirm that the data being collected from employees does not fall within the scope of these laws.

6.2.1 US Privacy Act of 1974

A more directly relevant federal law for US airports is the US Privacy Act of 1974. The US Privacy Act details important rights and restrictions on data held by US government agencies, and impacts how TSA and CBP collect data at airports. It created a broad set of expectations among the general public and employees regarding how organizations should protect their data.

Although the law predates biometrics and the internet, it established a framework for data privacy and protection that many subsequent federal, state, and local laws follow. Some of the key concepts established by the law include:

- US citizens have the right to access any data held by government agencies, and a right to copy that data.
- US citizens have the right to correct any information errors.
- Agencies should follow data minimization principles when collecting data—collecting the least information "relevant and necessary" to accomplish its purposes.
    - Access to data is restricted on a need-to-know basis (for example, employees who need the records for their job role).
    - Sharing of information between other federal (and non-federal) agencies is restricted and only allowed under certain conditions.

6.3 State Data Privacy and Biometric-Related Legislation

At the state level, there are a number of relatively new privacy, biometric, and data protection-related regulations and laws.

As of January 2021, at least six states (California, New York, Maryland, Massachusetts, Hawaii, and North Dakota) had passed some type of data privacy and data protection laws, and at least one other (Illinois) had passed laws specifically regulating the use of biometrics.

While a detailed analysis of each of these laws is beyond the scope of this project, we highlight several that have provisions that may be relevant to airports considering an ACS transition.

6.3.1 New York State SHIELD Act

In 2019, New York passed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which requires "any person or business that owns or licenses computerized data which includes private information of a resident of New York" to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information." The law's provisions can apply to businesses outside of New York, for example, if they collect PII from a resident of New York. It also requires covered entities to follow more stringent data breach notification requirements.[18]

[18] Pillsbury Law, "New Cybersecurity and Privacy Law in New York Affects Employers in New York and Beyond," https://www.pillsburylaw.com/en/news-and-insights/new-cybersecurity-and-privacy-law-in-new-york.html.

6.3.2 California Consumer Privacy Act

In 2018, the California Consumer Privacy Act (CCPA) was signed into law. The CCPA has been called the most comprehensive internet-focused data privacy legislation yet enacted in the US, and has no equivalent at the federal level.

Under the CCPA, consumers have a right use a Data Subject Access Request (DSAR) to access the categories and specific pieces of personal information held by covered businesses. The CCPA broadly defines personal information as, "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The CCPA includes a list of identifiers that are considered personal information, including biometrics, geolocation, email address, browsing history, and employee data.

In 2020, the law was amended to exempt employee personal information from most of the CCPA's protections until January 1, 2022. However, based on the literature review for this report, it appears that while employees are temporarily excluded from most of the CCPA's protections, two areas of compliance remain that could be relevant to airports. Specifically, the CCPA requires employers to notify employees at the time PII is collected, and it requires employers to maintain reasonable safeguards for a subset of personal information. If a business fails to maintain those reasonable safeguards and a data breach occurs, individuals affected by the breach have a private right of action against the company.

6.3.3 Illinois Biometric Information Protection Act (BIPA)

Passed into law in in Illinois in 2008, the Biometric Information Protection Act (BIPA) was intended to address the heightened risk of identity theft associated with the processing and storage of biometric data. The legislature's findings state that, "unlike other unique identifiers that are used to access finances or other sensitive information," when biologically unique data is compromised, "the individual has no recourse," because the individual cannot change these identifiers.

BIPA excludes certain types of entities, including financial institutions subject to the GLBA of 1999, governmental entities and agencies, and contractors to governmental entities or agencies. These exclusions would appear to apply to airports that are part of a local government, although an airport should confirm that with legal counsel.

Some key provisions of BIPA are highlighted below because they may be incorporated into future regulations that do impact airports, and therefore may factor into future planning considerations for airport ACS.[19] BIPA establishes several key definitions:

- "**Private entity** means any individual, partnership, corporation, limited liability company, association, or other group, however organized."
- "**Biometric information** means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of 'biometric identifiers.'"
- "**Biometric identifier** means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." The law expressly excludes certain data elements from this definition (e.g., writing

[19] "The Illinois Biometric Information Privacy Act ("BIPA"): When Will Companies Heed the Warning Signs?," *The National Law Review*, Volume X, Number 48, https://www.natlawreview.com/article/illinois-biometric-information-privacy-act-bipa-when-will-companies-heed-warning.

samples, photographs, tattoo descriptions, information captured in a health care setting or under HIPAA, etc.)

BIPA imposes the following obligations on businesses that collect and store biometric information:

- **Written retention and destruction policy:** Private entities in possession of biometric data must develop a written policy (made available to the public) establishing a retention schedule and guidelines for permanently destroying biometric data.
- **Written release:** Private entities are prohibited from obtaining biometric data without informed written consent.
- **Prohibition against profiting (even with consent):** Private entities in possession of biometric data are prohibited from selling, leasing, trading, or otherwise profiting from that biometric data.
- **Restrictions on disclosure:** Private entities in possession of biometric data may not "disclose, redisclose, or otherwise disseminate" it unless consent is obtained or the disclosure is required for specific purposes (e.g., the disclosure is necessary to complete a financial transaction, required by law, or pursuant to a valid warrant or subpoena).
- **Security requirements:** A private entity in possession of biometric data must use reasonable standards of care applicable to the entity's industry and in a similar, if not more protective, manner as the entity uses for other confidential and sensitive information (defined by reference to a list of elements that includes, among others, SSN, passcodes, and account numbers).

BIPA includes a "private right of action" (i.e., the right for private individuals to sue) that enables any person to recover damages for negligent, intentional, or reckless violations.

6.4 Future Legislative Trends Related to PII, Data Protection, and Privacy

A growing number of state and local governments are considering restrictions on the collection of biometric and other data. It is important for airport managers to monitor their state and local legislative activity on a regular basis.

In terms of potential federal data privacy and biometric-related activity, a number of legislative proposals bear monitoring in the next few years:

- The **Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act)** would have required companies to obtain express consent before processing sensitive data or using personal data for behavioral or psychological studies; it would have provided data portability, as well as given users the right to access, correct, and delete their data.
- The **Data Broker Accountability and Transparency Act of 2020 (DATA Act)** would have provided individuals with a right to access their data, dispute that data's accuracy, and opt out of the use of their data for marketing purposes.
- The **Data Protection Act of 2020** would have created an independent national Data Protection Agency that would have been empowered to promulgate rules and initiate enforcement actions to protect individual privacy, thus taking enforcement out of the Federal Trade Commission's hands.
- The **Data Accountability and Transparency Act of 2020** would have banned the collection, use, and sharing of personal data in most circumstances.

- The **Ethical Use of Facial Recognition Act** would have placed a moratorium on the use of facial recognition technology by the federal government until Congress passed legislation regulating its use.
- The **Facial Recognition and Biometric Technology Moratorium Act of 2020** would have barred the federal government from use of biometric technology; the ban could only be lifted through a subsequent act of Congress.
- The **National Biometric Information Privacy Act of 2020** would have prohibited private companies from collecting biometric data without consumer or employee consent.

At a minimum, airport managers undertaking an ACS transition should consider the following questions during the Project Planning and Future Planning phases:

- What is the absolute minimum PII needed? How can my airport avoid or minimize the collection, storage, and processing of PII in my ACS?
- If my airport were required to document exactly how and when airport employee PII is collected, stored, and processed by the ACS, could I provide that data in a timely manner? If there are changes to how PII is handled, are those changes documented as well?
- If my airport ACS were required to demonstrate reasonable safeguards against hacking, unauthorized data breaches, and other cybersecurity attacks, how would I do this?

SECTION 7: CONCLUSIONS

Given the complexity, cost, security, and operational impacts of implementing a new or upgraded ACS, airport operators and security managers must consider multiple, often competing, factors that may influence the decision-making process, project planning, and project completion. Airports and their stakeholders should use a rigorous process that considers the affected community and user experience; aligns with available budget and operating requirements; and is flexible enough to consider routine feedback, adjust for modifications throughout the transition period, and support future modifications and incorporation of new and emerging technologies.

Keys to success during the ACS Transition Process include:

- Defining relevant stakeholders and end users prior to beginning the ACS Transition Process helps to avoid unexpected challenges during the different phases of the process.
- Understanding future IT trends helps ensure the system is reflective of the most current technology capability at the implementation stage.
- Aligning requirements to available budgets can be a significant challenge, and must be considered before project execution.
- Preparing and regularly maintaining documentation will help ensure that system as-builts and other relevant documents remain current and can support decision-making over time.
- Consultants, integrators, and manufacturers must have both depth and breadth of airport-specific experience with ACS transitions, and collaboration between the entities should be robust.
- An experienced project manager should be identified, and the schedule of the ACS Transition Process should be audited routinely to stay on target.
- Defining needs of the system up front can help inform decisions regarding vendor and system selection.
- Seeking input from airport partners, stakeholder organizations, and other support systems helps ensure that the system will meet the needs and expectations of all operators and users.

APPENDIX A: LITERATURE REVIEW

The LAM LHA team performed an in-depth literature review of documents discussing current practices, guidance, and strategies regarding airport ACS. The review encompassed published documents including federal laws, federal guidance, academic research, ACRP and PARAS reports, documents written for the aviation industry, and non-airport documents.

The LAM LHA team also attended industry conferences and association committee meetings that addressed the topic of airport access control. Some of the information from the literature review was gathered from vendors' websites, white papers, and webinars, but the information presented in the final document is vendor agnostic and does not reference a brand or company name.

The following report presents the findings of the literature review, in the form of an annotated bibliography. This bibliography may also serve as a reference list for airport managers. Materials are presented by title, in alphabetical order.

Government Reports, Academic Literature, Guidance Documents

Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates. US Government Accountability Office (GAO). May 2016.

Summary: GAO was asked to review TSA's oversight of airport perimeter and access control security as it had last reported on the topic in 2009. This report mainly focuses on the extent to which TSA has assessed the components of risk and taken actions to oversee and facilitate security. GAO analyzed relevant past documents and data provided by the TSA and found that the methods used to conduct risks and vulnerabilities assessments need to be updated and improved. The report provides six main recommendations that would enhance airport perimeter and access control security, thereby mitigating threats to the system

America's Airports: The Threat from Within. House Homeland Security Committee Majority Staff Report. February 2017.

Summary: This report came in response to several well-publicized insider threat incidents involving airport and airline employees violating or subverting security requirements. The report found that the majority of airports do not have full employee screening at secure access points, there are multiple gaps in the data collected, and issues in accessing sensitive areas in airports and related infrastructure. The report makes several recommendations that are relevant to airport ACS, including the need for continuous and timely vetting of airport employees who receive access to secure areas of the airport, and more stringent regulations and standards for auditing and controlling the use of security credentials.

A Review of Access Control Measures at Our Nation's Airports. Subcommittee on Transportation Security Committee on Homeland Security House of Representatives. February 3, 2015, and April 30, 2015. https://www.govinfo.gov/content/pkg/CHRG-114hhrg94105/html/CHRG-114hhrg94105.htm.

Summary: Following the misuse of a SIDA credential by an airport employee in December 2014, the Aviation Security Advisory Committee (ASAC) reevaluated airport employee screening protocols. The ASAC proposed improving employee vetting procedures, the creation of a database of individuals with revoked credentials, and a limit on the number of access points to Sterile Areas in the airport. Within days of the ASAC recommendations, the DHS Secretary took action to enhance

security by requiring the screening of airport employees when they travel and increasing random airport employee screening.

Biometric Recognition: Challenges and Opportunities. National Research Council. 2010. https://doi.org/10.17226/12720.

Summary: A general "systems" analysis of biometrics that describes the inherent strengths and limitations of the use of biometrics, and presents frameworks for policy makers and others to apply. Not specific to aviation or airports.

Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control. US Transportation Security Administration. 2015.

Summary: The ASAC was asked by TSA to recommend security measures for screening, vetting, and access control of airport employees. In the section entitled "Internal Controls and Auditing of Airport-Issued Credentials," the report listed recommendations related to improving access control at airports, such as increased random checking of credentials, the use of biometrics in access control media, and, where operationally feasible, reducing access points between secure and non-secure areas of the airport. The report is useful for airport operators transitioning to a new ACS in that it highlights that effective ACS is not only a technology challenge, but must be backed by appropriate airport security policies and procedures.

Fort Lauderdale-Hollywood International Airport Active Shooter Incident and Post-Event Response After-Action Report. Broward County Aviation Department. August 2017.

Summary: This report provides recommendations to the Broward County Aviation Department in the aftermath of an active shooter incident in January 2017. Although the incident was not the result of a breach in an airport ACS, the report made several recommendations that are relevant to ACS design and implementation, such as the importance of being able to provide access credentials on an emergency basis to first responders, the ability to support unified communications in the aftermath of a security incident, and the requirement to have roles and responsibilities clearly defined in the event of a security incident.

Fusion of Security System Data to Improve Airport Security. National Research Council. 2007. https://doi.org/10.17226/11913.

Summary: This report describes the multiple ways in which different types of security sensor, biometric, and other data can be fused to improve airport security. It provides useful general guidance on designing security systems that integrate multiple sources of data. Chapters 3 and 4 of the report specifically address airport ACSs. However, the report focuses heavily on biometric technology and is from 2007, which limits its relevance to many US airports.

Guidance for Airport Perimeter Security. National Safe Skies Alliance – Program for Applied Research in Airport Security. December 2018.

Summary: Describes principles, measures, and implementation considerations to address perimeter security at airports of various types and sizes. The guide explains the need for perimeter security and principles such as layered security. Categories of perimeter security—physical, electronic, and operational—are defined. The report discusses the advantages, disadvantages, and applicability of different solutions given varying airport environments. The report is relevant to ACS in two respects: first, it describes ACS requirements and technologies related to perimeter security (e.g., pedestrian portals); second, it provides a framework for transitioning to a new perimeter security system. This framework has elements that can be applied to transitioning to a new airport ACS.

Guidance for Airport Security Master Planning. National Safe Skies Alliance – Program for Applied Research in Airport Security. January 2019.

Summary: Provides guidance and planning tools for developing and implementing an airport Security Master Plan, which enables an airport to forecast future security needs and associated costs. The document defines a process for Security Master Plan creation: scoping; understanding existing conditions; addressing functional security areas and technologies; development and action (implementation) phase; and monitoring and maintenance. Appendix E of the report contains a useful framework for capturing existing conditions related to ACS and for prioritizing improvements to an ACS relative to other airport security plan initiatives.

Guidance for Protecting Access to Vital Systems Impacting Airport Security. National Safe Skies Alliance – Program for Applied Research in Airport Security. 2017.

Summary: This guidebook provides airport operators with a framework for understanding the systems that are vital to airport security, how to apply a risk strategy to each system using security controls, and guidance to ensure that these security controls are effective. The airport systems discussed include airport LAN and Wide Area Network infrastructure; Video Surveillance Systems; Perimeter Intrusion Detection Systems, and Network Security Management Systems. Section 4.5.9 provides a two-page discussion of PACS. Given the space constraints, the discussion is limited to a definition and functional description of the components of an airport ACS, and brief descriptions of technologies used in airport PACS, such as biometrics, card readers, and REX devices.

Impact of Regulatory Compliance Costs on Small Airports. National Academies of Sciences. Engineering, and Medicine. 2013. https://doi.org/10.17226/22581.

Summary: Chapter 5 of the report presents survey data from small US airports on the type of ACS they have installed, as well as the cost of these systems. Therefore, while the report is dated, it is only third-party research report the team identified that focuses specifically on ACSs for small airports, and provides empirical ACS cost and technology adoption data, which may be useful to small airport operators.

Insider Threat Roadmap 2020. Transportation Security Administration. tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf.

Summary: This document defines insider threats and provides a plan to guide the TSA's effort to mitigate insider threats. The TSA identifies long-term trends and patterns associated with insider threats through a threat assessment that highlighted incidents involving airport employees between 2014 and 2019. A series of guiding principles, including promoting a security culture, achieving unity of effort across the transportation industry, and creating operational efficiencies that allow for reinvestment in security, describes the way in which the TSA could navigate the risk terrain of implementing an insider threat mitigation vision. The roadmap concludes by offering a series of strategic priorities, including promoting data-driven decision-making, advancing the operational capability of TSA, and maturing the capability of the Transportation Systems Sector.

Integrating Airport Information Systems. National Academies of Sciences, Engineering, and Medicine. 2009. https://doi.org/10.17226/14234.

Summary: For each major airport functional area (including security), this document describes the business-critical information, data elements, metrics, and data sources needed for that functional area's information system. The relevant section of the report is Chapter 4, which contains a discussion of how information systems impact airport security, including access control.

Recommended Security Guidelines for Airport Planning, Design, and Construction. National Safe Skies Alliance – Program for Applied Research in Airport Security. 2017.

Summary: This report discusses airport ACS within a larger context of other airport security requirements and processes, such as baggage inspection, perimeter security, and checkpoint security. Integrating security systems and operations into the planning and design of airport construction and refurbishment projects can be a very complex task. This publication is intended to help mitigate challenges by focusing on various airport security planning and design issues in airside, landside, terminal, perimeter, IT, surveillance, access control, and the unsecured side of the airport. Section 10 focuses specifically on airport ACSs, and includes brief discussions of regulatory requirements, IT system integration, ACS technology trends, and other associated topics.

Securing Our Skies: Oversight of Aviation Credentials. Testimony by TSA Deputy Assistant Administrator Darby LaJoye, before the House Committee on Oversight and Government Reform, Subcommittee on Transportation and Public Assets. February 3, 2016.

Summary: This testimony emphasized TSA's role in airport access control and aviation worker credentialing at US airports. LaJoye updated the committee on the progress TSA had made in reducing risks associated with insider threats at airports across the nation. He reported an increased number of employee screenings in 2015, a reduction of access points in 88 percent of airports across the US, successful collaboration between the TSA's Insider Threat Unit and federal partners, and the continued implementation of ASAC recommendations. He also stressed the TSA's commitment to vetting and credentialing workers in the aviation sector, the TSA's security program requirements, and the TSA's authority to conduct inspections, assessments, and audits of airport access control plans.

Security at Airports. Airport Council International (ACI) Policy and Recommended Practices Handbook. November 2016.

Summary: In this guidance document, ACI issued recommendations aimed at avoiding the inappropriate use of access control. ACI recommended that security restricted areas be established at each airport, and that the separation between restricted areas and other areas be clearly defined so that only authorized personnel could enter. ACI also recommended that persons who have not undergone background checks be escorted at all times within the security restricted area, while staff issued with identification cards should be subject to periodic background re-checks by the relevant government authorities to ensure their validity.

SIDA Airport Security Fiscal Year 2017 Report to Congress. Transportation Security Administration. February 6, 2018. https://dhs.gov/sites/default/files/publications/TSA - SIDA Airport Security.pdf.

Summary: This report concerns the misuse of SIDA credentials, and the TSA details the steps it has taken to ensure the security of SIDAs. The report emphasizes the measures taken by the TSA to enhance aviation security and decrease the risk of SIDA abuse. These measures include aviation worker vetting programs, coordination with the FBI's Rap Back service, the TSA's Insider Threat Program, regulatory compliance efforts, airport self-vulnerability assessments, and routine SIDA audits and compliance checks.

Staff Access Control at Airports, Bite, Katalin Emese. Periodica Polytechnica Transportation Engineering 38 (2010): 9-12.

Summary: This document provides an overview of US and international aviation security incidents related to staff access control, and reviews advantages and disadvantages of various technologies and approaches for access control.

Standards for Airport Security Access Control Systems, Radio Technical Commission for Aeronautics (RTCA). 2019.

Summary: This comprehensive reference document provides detailed guidance related to the operational and technical requirements of airport ACSs. It discusses these components at length: communications systems; credentialing and identity management, including biometrics; and VSS. In its technical section, the authors present the most recent information related to technical performance standards for ACS technologies and emerging technology trends. Furthermore, it offers airport operators practical checklists and prescriptive guidance intended to reduce the risks and costs associated with procuring, designing, and implementing an effective airport ACS. It is particularly helpful in explaining the interrelationships and interdependencies between components and subsystems of an ACS, and in providing guidance on how these components can be integrated effectively and controlled via a Security Operations Center.

Strategies for Effective Airport Identification Media Accountability and Control. National Safe Skies Alliance – Program for Applied Research in Airport Security. 2019.

Summary: ID media issued by airports to employees, contractors, and other individuals are an important component of an airport ACS. This report focuses on processes and best practices for ensuring appropriate control and accountability over these identification media. Section 11 of the report discusses how ACS and IDMS can be used to assist in the auditing and validation of ID media.

Transportation Security: Issues for the 116th Congress. Elias, Bart. Congressional Research Service, 2019. https://fas.org/sgp/crs/homesec/R45500.pdf.

Summary: This report describes major transportation security issues facing US legislators, including aviation security. The report includes sections on recently passed US federal legislation related to screening and vetting of airport employees, and securing public access areas in US airports. The report also describes some of the regulatory requirements these laws place on US airports and other regulated parties.

TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals. US Government Accountability Office. February 2020.

Summary: GAO was asked to review current TSA and aviation stakeholders' efforts to mitigate insider threats at airports. The study evaluated the different efforts made by airport operators and carriers to mitigate insider threats in airports, along with investigating TSA's Insider Threat Program to determine if it is appropriately guided by a strategic plan and achieves its goals. The report established that the TSA's Insider Threat Program is not guided by a strategic plan with strategic objectives, and it does not have performance goals. Therefore, GAO recommended improvement of the program and the establishment of real and achievable goals to limit insider threats.

TSA's Efforts in Enhancing Airport Access Control. Statement by Melvin Caraway, Acting Administrator, Transportation Security Administration, US Department of Homeland Security before the House Committee on Homeland Security, Subcommittee on Transportation Security, Thursday, April 30, 2015.

Summary: In his statement before Congress, Administrator Carraway focused primarily on the TSA's efforts to mitigate insider threat at airports around the United States. The ASAC had previously identified five ways that the TSA could address vulnerabilities in its control of access to the Sterile side of an airport and mitigate insider threats at an airport. These measures included security screening and inspection, airport employee vetting and security assessments, internal controls, auditing of airport-issued credentials, risk-based security for high-risk populations and intelligence, and security awareness and vigilance. Carraway expressed his commitment to reviewing and implementing these measures, and reported that the TSA had already begun to require increased CHRCs for airport employees, require screenings for airport employees before travel, reduce access points to secure areas to an operational minimum, and increase airport employee screening to include random screenings throughout the day.

Regulatory and Legal

49 CFR § 1542.207 Access Control Systems (updated on June 26, 2020)

Summary: This legislation outlines required measures for controlling entry into the Secured Areas or the Airport Operations Area (AOA) of an airport. Measures include ensuring that only individuals that are authorized to have unescorted access to the Secured Area are able to gain entry into area, ensuring that individuals are immediately denied entry to Secured Areas when their access authority is withdrawn, and providing a means to differentiate between those who have access to an entire Secured Area and those who only have access to a specific portion of the area. Further elements of the legislation include a stipulation that an airport may propose alternative security measures to those outlined above, as long as the measures provide an equal overall level of security. If approved by TSA, these would be incorporated as amendments to the Airport Security Program. Additionally, the code allows an airport operator to issue a second access medium to an individual who has unescorted access to Secured Areas or the AOA but is temporarily not in possession of the original access medium.

49 CFR § 1542.211 Identification Systems (updated on June 26, 2020)

Summary: This regulation outlines procedures concerning personnel identification systems. Personnel identification systems must include media that conveys a full-face image, full name, employer, and identification number; clearly indicates the scope of the individual's access privileges; indicates an expiration date; and is of a sufficient size as to be readily observable. The code also ensures accountability through measures such as retrieving identification media from those who no longer have unescorted access authority, reporting missing identification media, securing media supplies, auditing the system at least once a year, and ensuring only one identification media is issued to an individual at a time. Airport operators must also establish a challenge program to check the authority of an individual who is not displaying proper identification. An escort procedure must also be established by airport operators.

FAA Reauthorization Act of 2018 (Public Law 115–254)

Summary: This Act contains provisions relevant to airport ACS, including clarification that TSA-led random inspections of aviation workers be targeted, strategic, and focused on providing the greatest level of security effectiveness. It also directs TSA to continue its covert testing of employee

access controls, and provide measures of the effectiveness of such operations to airport operators, and as appropriate, to airlines. The Act also establishes more stringent standards for individuals applying for SIDA access, requiring that such individuals provide their SSN in order to strengthen vetting effectiveness.

Aviation Employee Screening and Security Enhancement Act of 2017 (H.R.876, 115th Congress)

Summary: This bill directs the TSA to conduct, and submit to Congress and the GAO, a study assessing the impact of airport employee access points from non-secured to secure airport areas. It also directs the TSA to work with a number of actors to enhance security awareness of credentialed airport workers regarding insider threats to aviation security, and identify best practices related to airport access controls. The bill dictates that the TSA shall identify advanced technologies for securing employee access to Secured and Sterile airport areas. The bill was received in the Senate and referred to the Committee on Commerce, Science, and Transportation.

FAA Extension, Safety, and Security Act of 2016 (Public Law 114-190)

Summary: This legislation outlines provisions relevant to airport ACS, including a requirement that TSA notify congressional committees of any Category X airport that was missing 3 percent (5 percent for Category I–IV airports) of their SIDA credentials. The law directed TSA to update the eligibility criteria and disqualifying criminal offenses for SIDA access credentials based on other transportation vetting requirements and knowledge of insider threats to security. The law proposes that TSA expand the criminal history look-back period, and that individuals be disqualified if they have been released from prison within 5 years of their application. The statute directs TSA to establish a formal waiver process for individuals who are denied credentials. It also calls for full implementation of recurrent vetting of airport workers with SIDA access credentials using the FBI's Rap Back service to identify disqualifying criminal offenses. In addition, the Act mandates that TSA develop a model and best practices for unescorted access security that uses intelligence, scientific algorithms, and risk-based factors; ensures integrity, accountability, and control; and subjects airport workers to random physical security inspections conducted by TSA representatives.

Gerardo Hernandez Airport Security Act of 2015 (Public Law 114-50)

Summary: This Act contains provisions relevant to airport ACS, including a requirement that airports adopt plans for responding to security incidents and create a mechanism for sharing information among airports regarding best practices for airport security incident planning, management, and training.