SAFE SKIES

PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0038

October 2022

Airport Guidance for Identity Management Systems (IDMS)

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

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

Gloria Bender
Andy Entrekin
Jessica Gafford
TransSolutions
Fort Worth, Texas

Saurabh Pethe
Kinexis Consulting
Parsippany, New Jersey

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 0038 PROJECT PANEL

Chris Cole *Dallas Fort Worth International Airport*
Paul Berumen *Phoenix Sky Harbor International Airport*
Antonella DeFilippis *Massachusetts Port Authority*
Arayna Hamilton *Jacksonville Aviation Authority*
Abedoon Jamal *San Francisco International Airport*
Dawn Lucini *Telos Identity Management Solutions*
Sarah Pilli *American Association of Airport Executives*
René Rieder *Burns Group*

AUTHOR ACKNOWLEDGMENTS

The Research Team would like to acknowledge the assistance of various airports, aviation stakeholders, and representatives from other critical infrastructure sectors in developing this guidance.

- National Safe Skies Alliance's PARAS, which provided funding. Particular thanks are given to the program manager, Jessica Grizzle.
- Keith Jackson, Tanna Almond – Hartsfield–Jackson Atlanta International Airport (ATL)
- Robert Boblitz, Aliesha Gomez, Nathaniel Tubman, Rick Thorne – Baltimore/Washington International Thurgood Marshall Airport (BWI)
- Antonella de Filippis, Nancy Pullen – Boston Logan International Airport (BOS)
- Mike Wahl – Dallas Fort Worth International Airport (DFW)
- Steve Guthrie – Friedman Memorial Airport (SUN)
- Jacob Graef, Doug Mansel – Oakland International Airport (OAK)
- Lauren Curtis – Seattle-Tacoma International Airport (SEA)
- Chris Cole, Yvette Santos – San Antonio International Airport (SAT)
- Abedoon Jamal – San Francisco International Airport (SFO)
- Mary Ouimet – Tampa International Airport (TPA)
- Sarah Pilli, Kyle Herbig – American Association of Airport Executives (AAAE)
- Dawn Lucini – Telos Identity Management Solutions, LLC
- Imran Rana – AlertEnterprise, Inc.
- Joseph DeGrassi, David Lenot – Genetec Inc.
- Russell Compton – HID Global
- Chris Cola, Mike Trilk – Honeywell
- David Peeples – Intellisoft
- Vik Ghai – Vector Flow
- Matt Powell – Convergint
- Calin Andronescu – MC Dean

CONTENTS

EXECUTIVE SUMMARY
PARAS ACRONYMS ix
ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS x
SECTION 1: INTRODUCTION 11
1.1 Identity Management Background 11
1.2 Research Approach 11
1.2.1 Literature Review 12
SECTION 2: ELEMENTS OF AN IDMS 13
2.1 Types 13
2.2 Components 13
2.2.1 Software 13
2.2.2 Hardware 13
2.2.3 Interfaces, Integrations, and Information Flow 14
2.3 IDMS Process Flow 16
SECTION 3: IDMS PLANNING 19
3.1 Assessing the Need for an IDMS 19
3.2 Pre-Procurement Considerations 20
3.3 Identification of the Existing Processes and Systems 21
3.4 Integration Considerations 22
3.5 IT Systems and Requirements 25
3.6 Data Reconciliation, Cleanup, Staging and Migration 26
3.7 Staff and Stakeholders 26
3.7.1 Project Staff 27
3.7.2 Stakeholders 27
3.8 Cost Considerations 28
3.9 Technical Requirements 28
3.10 Operational and Process Requirements 30
SECTION 4: IDMS PROCUREMENT 32
4.1 Procurement Documents 33
4.2 Vendor Evaluation and Selection 35
4.3 Scope of Work Development 36
4.4 Submittal and Documentation Requirements 37
4.4.1 Project Quality Management 38
4.4.2 Coordination Meetings 39
4.4.3 Stakeholder Engagement 39
4.4.4 Warranty Requirements 39
4.5 Contract Considerations 39

SECTION 5: IDMS IMPLEMENTATION **40**
5.1 Schedule and Key Milestones 40
5.2 Environments 41
5.3 Data Migration 41
5.4 Testing and Cutover 42
5.5 Training 44
5.6 Project Closeout 45
5.6.1 Maintenance 46
5.6.2 End-of-Life Considerations 46
SECTION 6: SUMMARY OF BEST PRACTICES **47**
SECTION 7: EMERGING TRENDS AND INNOVATION **50**
REFERENCES **52**
APPENDIX A: INTERVIEW PARTICIPANTS **A-1**
APPENDIX B: INTERVIEW QUESTIONS **B-1**

TABLES & FIGURES

Figure 2-1. IDMS Database Date Sources and Outputs Diagram 15
Figure 2-2. IDMS Process Flow – New Badge Applicant 16
Figure 2-3. IDMS Process Flow – Renewal Applicant 17

EXECUTIVE SUMMARY

An Identity Management System (IDMS) is a tool that can benefit airports by streamlining and enhancing the credentialing processes and interactions between disparate systems. An IDMS can also enforce processes and procedures and improve compliance aspects associated with credentialing (i.e., audits and reporting). However, the time, effort, and cost to implement and maintain an IDMS can be significant, and it important to approach such a project with as much information as possible.

This document was developed to provide airports with information and guidance for implementing an IDMS. The information is organized following the process, from initial considerations and needs assessment through planning, procurement, and implementation.

The guidance is based primarily on the information and experiences gathered through interviews with airports, IDMS vendors, consultants, integrators, and service providers. Key lessons learned and best practices were derived from these contributors' real world experiences.

The following key considerations were identified:

- An IDMS may not be the best solution for all airports. The need for an IDMS should be carefully evaluated before any move to procure and implement a system.
- IDMS procurement requires careful planning and preparation.
- System procurement and implementation will typically demand a significant allocation of time, staff, and other resources.
- IDMS implementation is likely to require adaptation of the airport's credentialing processes.
- Implementation of an IDMS is not typically a one-time cost to the airport. It will require long-term support by IT personnel, the provisioning of a dedicated test environment, and ongoing training.
- The more a system is customized, the greater the risk and the cost to the airport.

Best practices identified during the interviews and research are presented at the end of major sections of the document. Key lessons learned are presented throughout the document in sidebars.

PARAS ACRONYMS

ACRP	Airport Cooperative Research Program
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
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
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

ACS	Access Control System
AI	Artificial Intelligence
CAD	Computer-Aided Dispatch
CBP	Customs and Border Protection
CBT	Computer-Based Training
CHRC	Criminal History Records Check
CMAR	Construction Manager at Risk
DAC	Designated Aviation Channel
FAR	Federal Aviation Regulation
FPRD	Fingerprint Results Distribution
GUI	Graphical User Interface
IDMS	Identity Management System
LAN	Local Area Network
ML	Machine Learning
PII	Personally Identifiable Information
PSAP	Public Safety Answering Point
PSIM	Physical Security Information Management
RAID	Redundant Array of Independent Disks
RFQ	Request for Qualifications
SLA	Service Level Agreement
SSN	Social Security Number
STA	Security Threat Assessment
VLAN	Virtual Local Area Network
VSS	Video Surveillance System

SECTION 1: INTRODUCTION

Airport credentialing is a critical element in maintaining the security of commercial service airports. The credentialing process has become increasingly complex due to growing badged populations, changing regulatory requirements, and the necessary interactions with a range of systems and services.

An Identity Management System (IDMS) is a tool that can streamline and enhance the credentialing processes and interactions between disparate systems. An IDMS can also enforce processes and procedures and improve compliance aspects of credentialing.

However, IDMS is a relatively recent option for airports and not as widely used as other airport security technologies. As a result, the issues to be considered when evaluating the need, costs, and benefits of an IDMS are not fully understood throughout the airport community.

This guidebook was created as a resource for airports to support informed decisions from evaluating the need for an IDMS through planning, procurement, implementation, and operation. The guidance is based on information and experiences gathered from U.S. airport projects of various sizes, and provides best practices and lessons learned to enable the most efficient and effective delivery of IDMS.

1.1 Identity Management Background

IDMS were originally developed for corporate and government applications to provide a single point for creating, managing, and closing out user identities. Prior to IDMS use, employee data was entered into different systems that each needed individual management (e.g., payroll, human resources, insurance, physical access control, IT access). This led to repetition in data entry that created more opportunities for errors. Recognizing this, vendors began developing IDMS to allow for a single identity record to be created and managed in a unified system.

Airports recognized the opportunity to use IDMS to provide a similar function within an airport environment. The IDMS industry developed aviation-specific workflows, and many of the functions used in commercial applications were eliminated or tailored to the particular needs of identity, security, and credentialing processes at airports.

It is important to understand that an IDMS is a supplement to access control and credentialing systems. It provides a framework of policies, processes, and system interfaces and integrations to manage and control user identities, and facilitates the collection and management of user information. Credentialing and access control systems can be operated individually without an IDMS, but IDMS is often a faster, more efficient process with better controls and accuracy.

1.2 Research Approach

Research for this guidebook consisted of a comprehensive literature review and interviews with individuals with experience in various aspects of IDMS. Information was collected to address a broad range of topics that pertain to initial consideration through planning, procurement, implementation, and operation of IDMS at an airport.

The research team communicated with organizations that have had direct involvement in the development, delivery, and operation of IDMS and related services in the commercial aviation environment. This included airports that are currently deploying or have deployed IDMS, IDMS vendors and integrators, a computer-based training provider, and both of the active Designated Aviation

Channeling (DAC) service providers. The organizations and individuals who participated in the interviews are listed in Appendix A and the interview questions are in Appendix B.

Interviewing both the users and the providers of the systems led to a comprehensive understanding of the different perspectives that may be encountered when assessing the need for, procuring, and implementing an IDMS.

1.2.1 Literature Review

The project team reviewed 28 documents from a variety of sources and industry perspectives. The literature included high-level discussions focused on the benefits of IDMS, academic work on specific aspects of systems and elements of IDMS, and governmental and regulatory documents that relate to IDMS without specifically defining the operations of IDMS.

While focused on access control systems (ACS), PARAS 0030 – *Guidance for Access Control System Transitions* is recommended as a companion read to this guidebook.[1] It details many direct links between ACS and IDMS, and identifies many of the same considerations and best practices for planning, procurement, and implementation.

The References section lists the literature reviewed for this guidebook.

[1] **PARAS 0030:** https://www.sskies.org/images/uploads/subpage/PARAS_0030.ACSTransitionProcess_.FinalReport_.pdf

SECTION 2: ELEMENTS OF AN IDMS

IDMS are built around software and hardware to manage and maintain the unique identity information that is used for credentials. To better understand IDMS, it is necessary to have some familiarity with the system's elements and what roles they play. This includes the software, hardware, typical integrations, and various processes and business rules that make the system operate as needed.

2.1 Types

There are two types of IDMS currently available on the market for airport applications: dedicated IDMS and unified IDMS.

Dedicated IDMS are standalone identity management solutions. Typically, they are ACS-agnostic, offer a wide range of integrations, and provide flexibility in the credentialing process.

Unified IDMS are typically offered as a module associated with an ACS. They are specific to the ACS vendor and generally will not work with an ACS provided by another vendor. These systems tend to offer a standard badging process with limited flexibility.

Both dedicated and unified IDMS provide additional capabilities over a traditional badging system. To determine the appropriate type of IDMS, an airport will need to consider cost, requirements, and the ACS currently implemented or planned for use at the airport.

2.2 Components

The major components of an IDMS include the software, hardware, and a set of interfaces and integrations that connect the IDMS to external services and systems. Vendors may use different names or terminologies for their particular product, but the information below is a generally applicable to all systems.

2.2.1 Software

At the core of an IDMS is software that performs three key functions: managing the process by which credentials are verified and granted; managing the assignment of rights to the badge holder; and managing the overall dataset that contains the badge holder's information, rights of access, and other associated information. These functions are supported by a database and an operating system that manages access and operations associated with the database.

The software is supplemented with additional tools such as those necessary for reporting and auditing, tracking the flow of credentialing, providing integrations to external services and resources, and providing a front-end interface for staff involved in the badging process.

2.2.2 Hardware

IDMS hardware typically includes workstations, servers, firewalls, and other elements required to run the system within the airport's IT governance. Equipment required will generally be determined by the specific IDMS selected.

The nature of the user interface and how the software is designed will likely impact the workstations. Workstation types include:

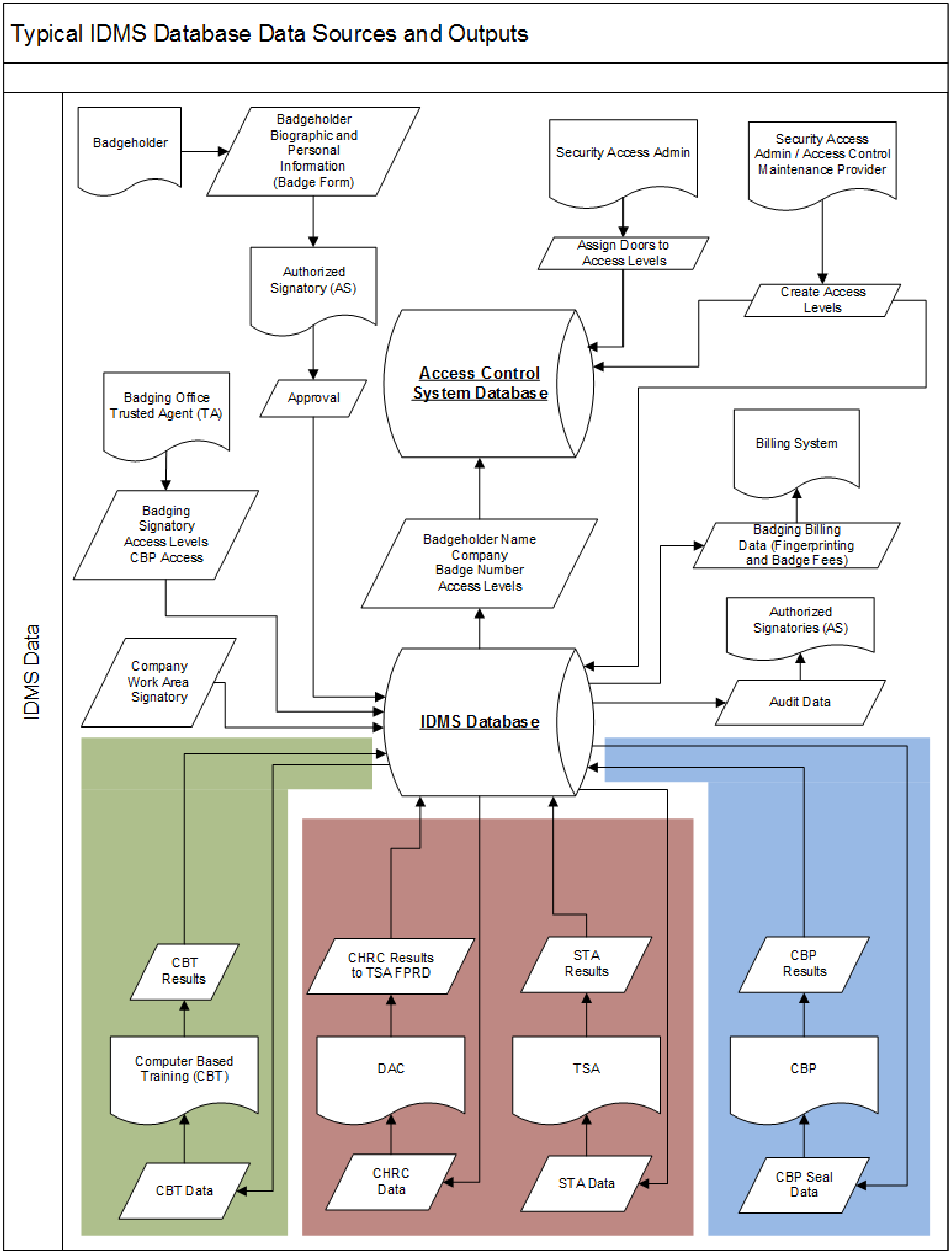
- **Web Portal:** Many IDMS offer a web portal to be used by Authorized Signatories to submit new badge applications or to renew existing badges. The web portal can be accessed through a standard web browser with the appropriate authentication. The functions are primarily data entry and report access. Information available via the web portal is generally limited to data considered suitable for the external-facing clients and personally identifiable information (PII) is typically protected. For example, an Authorized Signatory may be able to enter and confirm a Social Security Number (SSN), but for subsequent reviews, the SSN will typically be redacted to show only the last four digits or to prevent viewing the number entirely.
- **Badging Workstation:** The badging workstation has traditionally been a dedicated computer with a badging software application installed. The badging workstation will typically have multiple peripherals attached, which may include a photo capture device, biometric enrollment equipment, badge printer and encoder, scanner for identity documents, and other devices as needed to support the badging process. Due to the number of peripheral devices connected and the drivers needed to support them, the workstation will often be dedicated to badging only. The computer will typically have additional USB ports or other interfaces to enable connection of all of the devices. Some airports also provide a multiscreen layout with a customer-facing touchscreen to allow for verification of data, entry of a PIN, or acceptance of the badge. This configuration may require additional monitor outputs. Badging licenses for IDMS are typically tied to the number of badging workstations.
- **Administrative Workstation:** The administrative workstation is used by the airport's badging office personnel to perform back-office functions (e.g., report generation). The workstation may access the IDMS database through an application installed on the workstation or through a web portal. Access to database information may be limited based on the user login rights, data availability, and data visibility restrictions. A dedicated workstation may be used if the IDMS is segregated or does not allow access from a shared-use computer.

Security requirements, including antivirus/antimalware software, should be established for all workstations that can access the IDMS. This will be easier to implement and maintain for the badging and administrative workstations that are owned and operated by the airport. Computers or tablets used by the Authorized Signatories may be more difficult to keep up to date. To ensure that no external threats can enter the IDMS environment through the web portal, it may be necessary to automatically logoff users after a specified period of inactivity and prevent transfer of files and links.

2.2.3 Interfaces, Integrations, and Information Flow

An IDMS is designed to be interfaced and integrated with many different systems. It is the central repository of identity information and provides for management and flow of data between different systems and services. The flow of data among systems will vary depending upon the needs of the airport and the systems that are present. Figure 2-1 provides an example of the data flows, integrations, and interfaces that may be part of an IDMS.

Figure 2-1. IDMS Database Date Sources and Outputs Diagram


Typical IDMS Database Data Sources and Outputs
IDMS Data
Badgeholder
Badgeholder Biographic and Personal Information (Badge Form)
Security Access Admin
Security Access Admin / Access Control Maintenance Provider
Authorized Signatory (AS)
Assign Doors to Access Levels
Create Access Levels
Access Control System Database
Badging Office Trusted Agent (TA)
Approval
Billing System
Badging Signatory Access Levels CBP Access
Badgeholder Name Company Badge Number Access Levels
Badging Billing Data (Fingerprinting and Badge Fees)
Authorized Signatories (AS)
Company Work Area Signatory
IDMS Database
Audit Data
CBT Results
CHRC Results to TSA FPRD
STA Results
CBP Results
Computer Based Training (CBT)
DAC
TSA
CBP
CBT Data
CHRC Data
STA Data
CBP Seal Data

2.3 IDMS Process Flow

The primary functions of the IDMS are processing new and renewal badge applications. Figures 2-2 and 2-3 provide examples of these processes.

Figure 2-2. IDMS Process Flow – New Badge Applicant

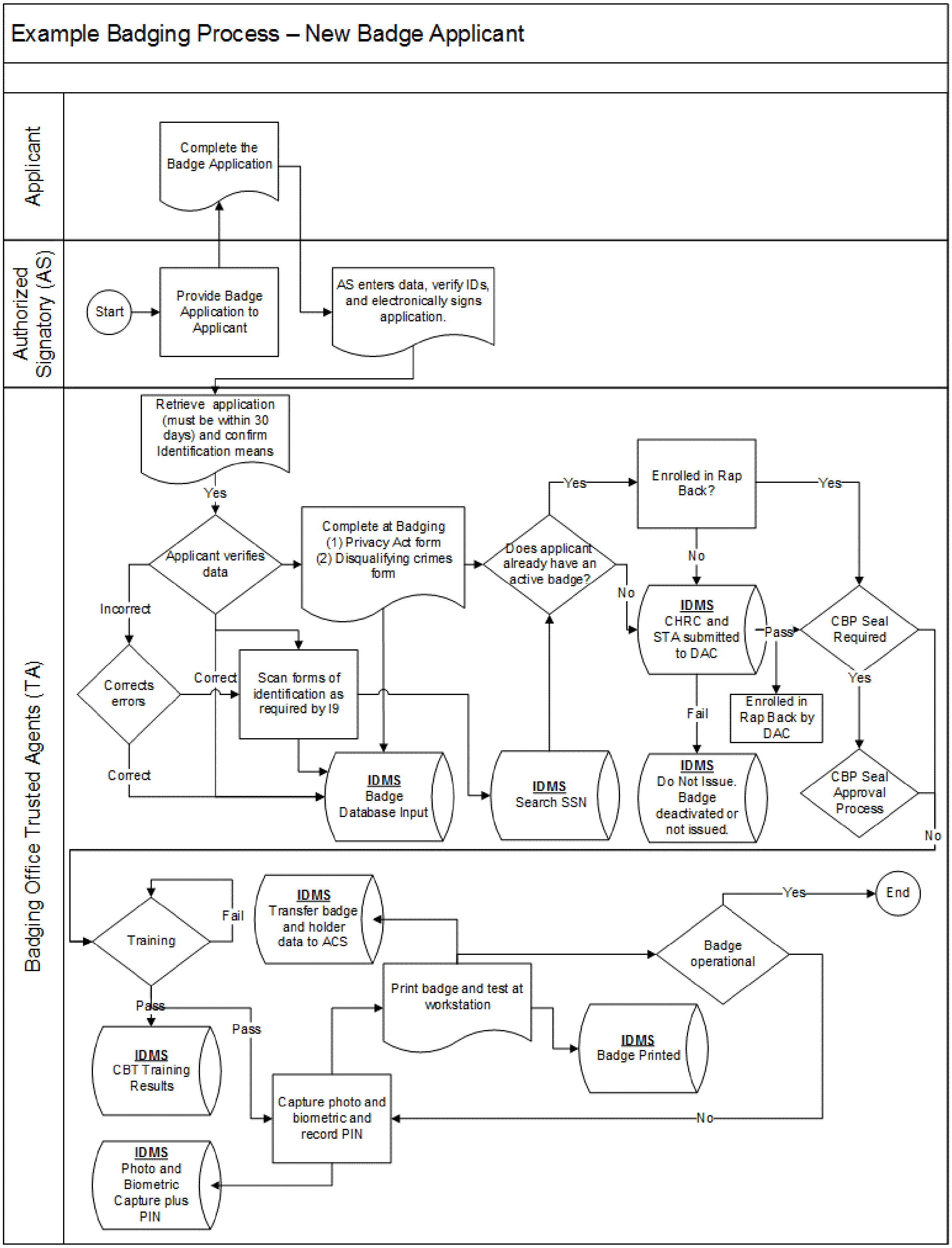
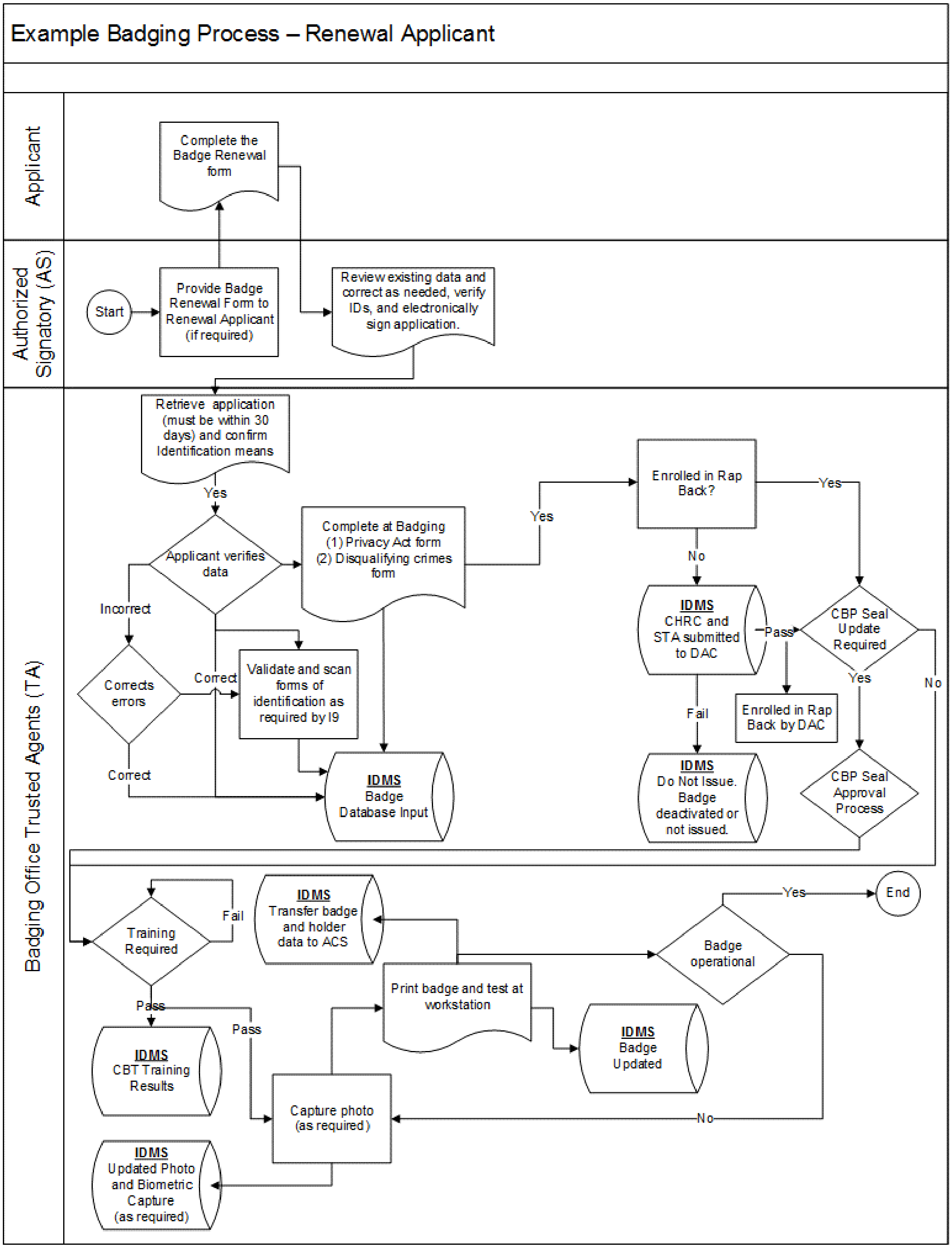

Example Badging Process – New Badge Applicant
Applicant
Authorized Signatory (AS)
Badging Office Trusted Agents (TA)
Complete the Badge Application
Start
Provide Badge Application to Applicant
AS enters data, verify IDs, and electronically signs application.
Retrieve application (must be within 30 days) and confirm Identification means
Yes
Applicant verifies data
Incorrect
Corrects errors
Correct
Correct
Complete at Badging (1) Privacy Act form (2) Disqualifying crimes form
Scan forms of identification as required by I9
IDMS Badge Database Input
Does applicant already have an active badge?
Yes
No
IDMS Search SSN
Enrolled in Rap Back?
No
Yes
IDMS CHRC and STA submitted to DAC
Pass
Fail
Enrolled in Rap Back by DAC
IDMS Do Not Issue. Badge deactivated or not issued.
CBP Seal Required
Yes
No
CBP Seal Approval Process
Training
Fail
Pass
Pass
IDMS CBT Training Results
IDMS Transfer badge and holder data to ACS
Print badge and test at workstation
IDMS Badge Printed
Badge operational
Yes
No
End
Capture photo and biometric and record PIN
IDMS Photo and Biometric Capture plus PIN

Figure 2-3. IDMS Process Flow – Renewal Applicant


Example Badging Process – Renewal Applicant
Applicant
Authorized Signatory (AS)
Badging Office Trusted Agents (TA)
Complete the Badge Renewal form
Start
Provide Badge Renewal Form to Renewal Applicant (if required)
Review existing data and correct as needed, verify IDs, and electronically sign application.
Retrieve application (must be within 30 days) and confirm Identification means
Yes
Applicant verifies data
Incorrect
Corrects errors
Correct
Correct
Complete at Badging (1) Privacy Act form (2) Disqualifying crimes form
Validate and scan forms of identification as required by I9
IDMS Badge Database Input
Yes
Enrolled in Rap Back?
Yes
No
IDMS CHRC and STA submitted to DAC
Pass
CBP Seal Update Required
Yes
No
Fail
Enrolled in Rap Back by DAC
IDMS Do Not Issue. Badge deactivated or not issued.
CBP Seal Approval Process
Training Required
Fail
Pass
Pass
IDMS Transfer badge and holder data to ACS
Yes
End
Badge operational
Print badge and test at workstation
IDMS CBT Training Results
IDMS Badge Updated
Capture photo (as required)
No
IDMS Updated Photo and Biometric Capture (as required)

Examples of processes and sub-processes that the IDMS will perform in addition to those listed above include:

- **Company Setup:** In order to start the credentialing process and assign an Authorized Signatory, it is first necessary to establish a company profile in the IDMS. The IDMS may be used to create company profiles by interfacing with an airport system that manages leases and contract information. The data may also be entered manually, either by the Trusted Agents in the badging office or by personnel in the airport's financial office. Once the company profile is created, the assignment and training of an Authorized Signatory can begin.
- **Criminal History Records Check (CHRC) and Security Threat Assessment (STA):** The CHRC and STA processes will typically occur through the DAC, with biographic information, fingerprints, and forms of ID submitted to the FBI and TSA. The results then are passed back through the DAC and captured in the IDMS.
- **Customs and Border Protection (CBP) Seal:** In order for an airport employee to access the CBP processing areas, a CBP seal is required as an endorsement on their badge. This seal request and approval process is often facilitated through the IDMS, either through the DAC or by allowing CBP to access the IDMS to review data electronically.
- **Computer-Based Training (CBT):** Training is required for most badge holders as part of the credentialing process. The IDMS often interfaces with the CBT system to enroll users, assign required training modules, and capture completion certificates and/or scores, as applicable.

SECTION 3: IDMS PLANNING

The work required to successfully implement an IDMS can represent a significant expenditure of time and financial resources. Upfront planning for the project results in more efficient delivery and greater success in meeting expectations for the system.

The following sections are heavily informed by interviews with airports and vendors, and represent recent experiences with the IDMS planning, procurement, and implementation process.

3.1 Assessing the Need for an IDMS

Before engaging in a major effort to procure an IDMS, the airport should perform a needs assessment to determine if an IDMS is a suitable solution. The benefits of an IDMS should be considered as part of the needs assessment. As reported by the airports interviewed for this research, some examples of the benefits include:

- Provides Authorized Signatories the ability to track the credentialing process
- Improves reporting processes and timeliness of reports
- Simplifies and expedites the auditing process
- Improves regulatory compliance in areas such as the credentialing process and badge termination
- Eliminates/reduces the need for manual or paper-based processes
- Eliminates/reduces storage of paper files
- Eliminates duplicate data entry by personnel in disparate systems (and the errors inherent in multi-entry)
- Eliminates the need to scan, control, and destroy paper records

Improvements in the badging process are not always guaranteed with an IDMS. Due to the nature of the various systems and the need to ensure that the proper steps are completed prior to issuing a badge, an IDMS could slow portions of the process. It is important to understand that checks and balances can introduce additional steps or procedures that could extend the processing time. However, an IDMS can offer advantages in many situations. The airport should consider the following points when determining whether an IDMS could offer advantages in their specific case:

- What is the status of the existing systems, services, and processes? If an IDMS is already in place, is it supported by the vendor and is the current end of life reasonable? Is the badging system or existing IDMS up-to-date? Has the system fallen several versions back, or is it not upgradable?
- How well do existing systems work? If the current approach is acceptable with the required levels of service and accuracy, an IDMS may not provide benefits that justify the cost and effort.
- How cumbersome is the existing process in terms of the demands on staff and processing time? An IDMS may be a worthy consideration if the current system and processes are slow and the time required to approve and deliver badges is unsatisfactory. It should be noted that this part of the assessment may determine that adding staff could solve this problem.
- How time consuming is it to manage and maintain the existing systems and processes? Does the existing solution require an excessive level of effort to keep running as required? This should consider internal airport staff as well as external support from vendors, contractors, or third parties.

- Based on IDMS on the market, are there features and services available that would be of benefit to the airport's credentialing operation? What, if any, customization is necessary or desirable in an IDMS?
- Do the existing system and processes meet requirements and standards, such as federal, cybersecurity, and data privacy (i.e., PII) requirements?
- What is the user and customer experience? Determining this could involve interviews or surveys of users to understand where there are problems or inefficiencies and where there are positive aspects. This will help inform the needs assessment to determine if an IDMS would be beneficial, as well as provide feedback to be considered when procuring an IDMS.

It is important to understand that a needs assessment is not an entirely objective process. There is not a specific formula or equation that will deliver a clear decision for whether to procure an IDMS. The airport must weigh the information gathered in terms of cost, benefits, and level of effort. The decision may also may be impacted by issues external to the credentialing process. For example, the decision may rest with a city, county, or state government with concerns or restrictions that the airport cannot directly influence.

IDMS may be beneficial in many situations, but they are not always essential. It is important to remember that a needs assessment may show that the investment is not necessary or practical under the current circumstances. This may be a matter of cost, complexity, or simply that the benefits are marginal and do not justify the effort. However, as the airport continues to grow and the badged population increases, an IDMS can be reconsidered.

3.2 Pre-Procurement Considerations

One of the most significant challenges in the pre-procurement phase is that most airports are not experts in IDMS. The research for this guidebook repeatedly indicated that it was crucial to gain an understanding of the particulars of IDMS, the manner in which they are defined and specified, and the options available on the market. Engaging consultants, vendors, and integrators can help overcome this challenge.

CONSULTANTS

Numerous airports noted that engaging a subject matter expert or consultant may be useful in implementation of a system. The consultant should have experience with IDMS capabilities, functions, and procurement, and an in-depth understanding of the regulatory and operational requirements for airport credentialing. A consultant can help manage stakeholder participation, review the expected badging process, identify the necessary integrations, assist with setting a realistic budget, and advise on the implementation schedule. The consultant should provide guidance based on experience and lessons-learned, help prepare procurement documents, provide information on the products available in the marketplace, and assist with setting up product demonstrations with possible vendors. The role of a consultant through the implementation will be discussed further in the appropriate sections.

VENDORS

For each IDMS under consideration, it is important that the airport have an understanding of its capabilities and features, see the user interface, and walk through the product process to determine if it is compatible with the airport's processes and procedures without requiring substantial customization. However, it is important to understand that the implementation of an IDMS will require compromise between the airport and the vendor. The airport will need to modify some of their procedures for the IDMS, and the IDMS will need to be configured to perform airport-specific functions.

The system manufacturers interviewed for this report recommended a product demonstration as part of either the pre-procurement or procurement process to help the airport understand the capabilities and limitations of the different products. The majority of the airports who participated in this research also recommended that the airport engage the IDMS manufacturers to familiarize themselves with the systems available on the market. A consultant can facilitate this engagement.

> **Lesson Learned:** Know what the vendor community offers before defining technical requirements.

INTEGRATORS

The use of an IDMS integrator varied among airports, and the airports noted specific situations or roles for which they would consider using an integrator. Scenarios and factors to consider include:

- **Current use of an integrator:** Many airports noted that they have a longstanding relationship with an integrator who is part of the security team. The integrator may already be responsible for maintaining other security systems such as the ACS and CCTVor video surveillance system (VSS). In many of these cases, the airport included the integrator in the implementation of the IDMS.
- **IDMS procured as part of a larger project:** Some airports stated that their IDMS was procured as part of a larger project, such as upgrades to the existing ACS or CCTV/VSS, or a major capital project, such as a concourse expansion. For these types of combined projects, an integrator will almost certainly be involved and may assist with the IDMS implementation. However, the airport often noted that while the the integrator was useful during construction, the airports often preferred to work directly with the IDMS manufacturer after implementation.
- **IDMS procured as a standalone project:** Where the procurement of the IDMS was a standalone project, airports generally agreed that the use of an integrator was dependent upon some external factors. The first was the level of staffing in the badging office. If the staff do not have resources or time to dedicate to the IDMS implementation, then the use of an integrator may be desirable during implementation. Also, if the IDMS implementation includes significant equipment replacement, then an integrator may offer some benefits. However, if the airport already has sufficient staff or a contractor to maintain the badging equipment, then an integrator may not be necessary.

3.3 Identification of the Existing Processes and Systems

The first step in planning an IDMS procurement is to identify the existing systems, processes, and procedures. Much of the information collected will help bidders or vendors understand the scope of work to be performed. This can lead to proposals that are more refined in terms of the level of effort required, the necessary vendor/contractor and airport resources, the schedule, and the cost to the airport.

> **Lesson Learned:** Document the existing badging process ahead of procurement.

Below are suggested steps for gathering the needed information:

- **Identify and document existing systems:** Identify existing identity management, badging, and access control systems. This should include documenting the make, model, versions, and all other pertinent data regarding hardware and software in order to assess and inform their ability to work with a new IDMS. The documentation should also include the number and locations of workstations associated with the badging process. This information, particularly the ACS make and model, will also identify options for a dedicated- or unified-type IDMS.

This effort should include verifying any end-of-life dates for software and hardware. It will be important to understand if any existing elements of the systems are scheduled to be discontinued, and to consider this in light of the IDMS procurement and implementation schedule.

- **Document existing security methods and systems:** Document the existing methods and systems/software used to ensure data security and resiliance, including cybersecurity tools and the means and methods for maintaining integrity of the data (e.g., redundant storage facilities).
- **Document the status/accuracy of the badging/identity dataset:** This includes understanding what information is collected, identifying inconsistencies or inefficiencies in the data, and developing an understanding of the magnitude and accuracy of the data stored. It is not uncommon for there to be duplicate and obsolete information in the datasets, and understanding the scale of this issue will help inform and refine the level of effort required to address it in advance of or during an IDMS procurement and implementation.
- **Document the existing workflow processes:** This includes the activities, actions, documentation, and entities involved in each part of the credentialing process. Detailed information is needed for what happens at each step, who is involved, and each step's precursors and successors.

  Documenting the existing processes and procedures is useful in identifying where things work well, and where there are inefficiencies that can be corrected as part of IDMS implementation. It is also useful in developing the scope of work for a proposal offering, assessing adjustments to staffing, and training staff in anticipation of process and procedural changes.
- **Identify and document existing integrations:** This should include the services and systems and their integration and interfaces to the badging process. Each of these interfaces will need to be assessed for their necessity and efficiency. The interface information will inform the procurement and delivery in terms of defining the scope of work and preparing for the transition of services.
- **Engage stakeholders:** This includes engaging the airport community to promote communication and collaboration throughout the process, and prepare for training and transition to the new system. It may also be useful to engage with the stakeholders to identify positive and negative aspects of the processes and system in order to address them as part of a procurement.

3.4 Integration Considerations

An early consideration in the planning for an IDMS is understanding and evaluating the integrations that are required between the IDMS and other systems, both internal and external to the airport. Based on previous IDMS implementations, the following integrations have been identified and should be considered as the system is planned.

It is important for an airport to identify the required system integrations prior to IDMS procurement so that the integration software (often APIs or gateways) is included in the system requirements. Not all vendors offer all integrations.

ACS

The most common integration of an IDMS is to the ACS. The IDMS will typically store all badge holder data, access levels, and badge information. The IDMS will be used to capture all of the biographic data for a badge holder and assigned access levels based on the individual's company and job classification.

The IDMS will capture the badge holder's photo and fingerprints and encode the badge. After the badge is produced, data from the IDMS will be transferred to the ACS to create the user profile in the access control database, link the badge holder to the encoded badge, and assign the appropriate access levels.

DAC

The next most common integration of an IDMS is to the DAC. The airport captures and submits the badge applicant's fingerprints and biographic data to the DAC for processing of the CHRC and STA. This integration allows for badge applicant data to be transferred directly from the IDMS to the DAC without the need for data re-entry, and allows for the receipt of the STA results. CHRC results are returned to the TSA Fingerprint Results Distribution (FPRD) website. An additional integration of the IDMS with the FPRD will be needed to obtain CHRC results and Rap Back notifications.

CBT

Another common integration is of the IDMS to the CBT system. This is often a bidirectional integration. The IDMS to CBT integration will create user names in the CBT and identify the courses to be completed. Once the user has completed the appropriate courses or training modules, the CBT system transfers the scores or completed status of the training back to IDMS, typically including the date and time that they were completed.

PSIM

At several airports interviewed, the IDMS is integrated with a Physical Security Information Management (PSIM). A PSIM is a top-of-system integration platform that manages the interaction of the various security systems and displays the geolocations all of the alarms and alerts in a single Graphical User Interface (GUI). The PSIM will typically use data from the ACS and CCTV/VSS, but if additional information on a particular badge holder is needed that is not in the ACS database, such as a cell phone number or supervisor contact, the PSIM will pull up that data from the IDMS for display to the PSIM operator.

CAD

At several airports interviewed, the IDMS is integrated with a Computer Aided Dispatch (CAD) system. A CAD system is often installed at airports that are Public Safety Answering Point (PSAP) facilities that receive 911 calls from the public. The CAD system typically includes a GUI that shows data on incoming calls, enables 911 operators to classify calls, and provides instructions and checklists for addressing different types of calls. Because PSAP facilities receive calls from mobile phones, most CAD systems also include a geolocation system to show the location of any cellular device associated with the call.

The CAD is primarily a PSAP tool, but many airports integrate the CAD to enable operators to also dispatch for airport functions, including security. The security integrations typically use data from the ACS and the CCTV/VSS, but if additional information on a particular badge holder is needed that is not in the ACS database, such as a cell phone number or supervisor contact, then the CAD will pull up data from the IDMS for display to the CAD operator.

HUMAN RESOURCES

The integration of the IDMS to human resources systems is fairly common outside of the airport industry. This integration is often used to pull basic biographic information to prevent the double entry of data. human resources can also provide an employee's job titles and other relevant information that allow for appropriate access levels to be assigned. The primary reason that the IDMS would be integrated with the human resources system would be to ensure that all access would be removed automatically if the person's status is changed within the human resources system. However, because only a small portion of the people in an airport's IDMS are employed directly by the airport (the majority of badge holders being airline and tenant personnel), airports often do not implement this integration.

TIME CLOCK AND ATTENDANCE

Some airports have integrated their IDMS with their time clock and attendance systems. This integration passes the badge holder and current badge information to the timekeeping system to enable the system to identify the badge for time clock and attendance purposes. The badge holder's role or job title can also be passed to the timekeeping system. Generally, the time clock and attendance system is integrated with other systems to report the hours, and the IDMS is only used to create the user and link the user to the badge. If the timekeeping system uses a biometric component, then the biometric could also be provided by the IDMS for a one-to-many comparison, or it could come from an encoded partition of the card if a one-to-one comparison is being performed.

ACTIVE DIRECTORY

The IDMS is sometime integrated with the Active Directory. Similar to Human Resources systems, this is most commonly used for airport employees who need access to airport systems. The intent of this integration is to remove access privileges in one of the locations and have them canceled in the other, regardless of which is primary.

FINANCIAL SOFTWARE

The credentialing process often has fees associated with certain steps that may be billed directly to a company. For example, background checks, new badges, and badge renewals are often charged to the company employing the badge applicant. An IDMS can be integrated with the airport's financial system to facilitate the direct transfer of billing information. However, as this can be a complex integration, many airports have elected to instead provide data in a spreadsheet format that can be imported into the financial system. Airports noted that a cost-benefit analysis should be performed prior to integrating with a financial system, as the interaction needed between the two systems is often fairly limited and may not be worth the cost.

CREDIT CARD PAYMENT SYSTEM

Some airports stated that their IDMS is integrated with a credit card payment system to capture the credit card payment record. However, as credit card systems are required to be in compliance with the PCI Data Security Standard, many airports and IDMS manufacturers have elected to not integrate the IDMS to the payment system, and instead rely on personnel to manually enter authorization numbers or mark items as paid.

APPOINTMENT SCHEDULING

Most of the airports noted the use of a scheduling system for badge office appointments, but this was typically not integrated with the IDMS. However, one IDMS manufacturer has a scheduling module available as part of the IDMS. If a scheduling system is not currently in use at the airport, having a scheduler provided as part of the IDMS may be considered an advantage during IDMS selection.

AVOID OVER-INTEGRATION

IDMS are designed to serve a particular set of functions. The airport should start with a clear understanding of their goals and requirements for the system, including justifications for each.

Care should be taken to avoid making the system overly complex or introducing functions and integrations that do not provide a clear benefit. For some systems and data flows, integration with the IDMS may appear to deliver benefits, but may unnecessarily complicate the system during its development and ongoing operation and maintenance. Every unique integration needs to be tested and maintained each time the IDMS or the integrated system is patched, debugged, or upgraded. Each of these creates a risk to the systems and their operation.

3.5 IT Systems and Requirements

The IDMS is a software system and, as such, will be implemented per an airport's IT governance in a manner that is similar to other software systems, though with the added complication of large amounts of PII within the IDMS. This requires that the system be secured to protect that data. The typical requirements include:

SYSTEM SERVER IMPLEMENTATION

IDMS server implementations varied across the airports surveyed, ranging from dedicated servers on site, to virtualized servers implemented within the airport's IT environment, to IDMS that were implemented entirely within the cloud. Regardless of the server type, all of the solutions were noted as being redundant with a stated Level of Service requirement. The solutions typically included redundant servers with storage configured so that a loss of one server would automatically failover and continue without loss of data. Regardless of the implementation type chosen, the metrics for high availability should be clearly defined and included in the procurement documents to ensure that the system will provide the proper level of redundancy.

SYSTEM STORAGE IMPLEMENTATION

Types of data storage also varied between airports. Some airports stored the IDMS data on the individual server hard drives. Other airports used Storage Area Networks or Network Attached Storage. A small number of airports used cloud data storage. All of the airports interviewed had some level of storage redundancy, with the storage often being configured in a RAID (Redundant Array of Independent Disks). All airports noted that data backups were also performed on a regular basis.

Regardless of the storage means selected, the storage should be sized to accommodate all IDMS data expected for the required retention period. While a typical database does not require a large storage capacity, the IDMS includes images and scanned documents that may occupy a significant amount of space. These can include the badge holder photograph and scans of identification documents such as driver's license, passport, birth certificate, etc. In addition, should adjudication be required, some documents related to the adjudication may also be scanned.

CYBERSECURITY VULNERABILITES

IDMS typically include integration to the DAC and a web portal for the Authorized Signatories. These allow access to the IDMS from outside of the airport's IT environment, which poses a potential cybersecurity vulnerability. Measures should be taken to monitor and protect these access points from cyber intrusion.

IT INFRASTRUCTURE

For the IDMS and other integrated systems within the airport's IT environment, the first consideration is whether these systems are currently on the same Local Area Network (LAN) or Virtual LAN (VLAN). Many airports have separate networks for security systems, and others have segregated the security systems using VLANs or other means to prevent access to the security systems. Generally, IDMS manufacturers stated that the airports provided the data security and connectivity between the IDMS and the various LANs and VLANs. It is important to consider the required connectivity so that the proper support is planned.

Similar to connectivity between the various LANs and VLANs, IDMS manufacturers stated that the airport provided connections for the web portal and to the DAC, and the manufacturer coordinated the implementation. Any certificates, firewalls, multifactor authentication, virtual private networks (including licensing) were provided by the airport. The airport will need to account for the resources and costs associated with these connections.

One additional factor to consider when implementing an IDMS is to ensure that any additional IT infrastructure required to support the system is included in the deployment plan. The airport should ensure that there are adequate network drops, network ports and switches, and bandwidth. Likewise, existing workstations, printers, and peripherals that are planned to be used to access the IDMS should be reviewed to determine if they are capable or if new devices should be procured. Often, the cutover strategy will dictate the provision of new workstations, peripherals, etc. The existing workstations will need to remain operational until immediately prior to the cutover, and they may continue to be needed as part of the fallback strategy should the IDMS cutover be unsuccessful. Airports often decide to retain the existing equipment until after the cutover is completed.

DATA SECURITY

The majority of the data stored within the IDMS is considered PII. The data collected as part of the badging process will include a person’s full name, address, SSN, date of birth, email address, phone numbers, and driver’s license number; in effect, every piece of information that would be necessary for identity theft. There may also be information included in the profile that indicates criminal history, adjudication, work permits, and resident status for foreign nationals. The security of the data needs to be assured, with the data encrypted while in rest and in motion. While IDMS typically provides encryption between the workstations and the servers, the overall security of the data and the encryption of the database is expected to be performed by the airport.

3.6 Data Reconciliation, Cleanup, Staging and Migration

IDMS and badging systems contain a significant amount of sensitive information, including PII and data related to security operations and systems in use at the airport. In the case of a large airport, there may be hundreds of thousands of individual pieces of data. The information and the dataset may vary widely in terms of quality, accuracy, and consistency, and may include duplications, out-of-date information, and errors.

The scale and quality of the existing datasets need to be assessed and documented in advance of the implementation. A plan should be developed to clean up the data, if required, before it is ported to a new system.

Airports stated that data migration was one of the biggest issues and sources of risk to a successful project, and that it was important to take the time and effort to reduce that risk. See Section 5.3 for detailed discussion of this topic.

Lesson Learned: Clean up the data before system implementation.

3.7 Staff and Stakeholders

There are two primary groups of personnel involved in the planning, procurement, and delivery of an IDMS. These are the staff required to implement the IDMS and the stakeholders who use the system as operators, supporters, or customers. Both groups need to be taken into consideration as the airport develops their IDMS solution.

3.7.1 Project Staff

The process of planning, procuring, and implementing an IDMS can place a significant demand on staff, including those necessary to execute the project and the support required from credentialing personnel. The demand on staff should not be underestimated when considering the procurement of an IDMS.

An early step in an IDMS project will be to assess the available personnel resources and their capabilities to support the project. This may in turn lead to identifying a need to hire additional staff, whether temporary, full-time, or on a contract basis. Many airports noted that IDMS projects took considerably longer than planned, which can also increase the burden on staff. The airport should ensure the following project staff are available:

- Project Manager with experience in running large, technically complex projects. Experience with IDMS, credentialing, and airport security systems are preferred. The Project Manager will have responsibility for keeping the project on track, managing schedules and personnel, and reporting progress to airport management or executives.
- IT and technical staff to support implementation of the technical elements of the system, support integration into existing systems, and otherwise assist in bringing the project to a successful conclusion.

Some airports retain the services of a consultant or consulting group to assist in managing the project, developing the technical requirements, and providing experienced support throughout the project life cycle.

3.7.2 Stakeholders

Implementation of an IDMS may affect many stakeholders. To ensure successful implementation, a comprehensive set of perspectives should be considered. The first step is to identify an appropriate cross-section of stakeholders that represents a variety of perspectives and requirements.

As the daily users of an IDMS, Trusted Agents (both management and workstation operators) will be crucial to the success of any implementation. It is especially important to consider their feedback if an IDMS will be replacing an existing system. These stakeholders have unique knowledge of everyday issues and inefficiencies that should be designed out of a new system. They are also an excellent resource to test the system.

Another set of stakeholders is the Authorized Signatories, who often act as gatekeepers to the credentialing process for potential badge holders, and bring a different set of requirements to consider. Potential changes to the Signatory’s tasks should be discussed. In addition, there will be more information available to the Signatory that will allow them to track the badges assigned to them, view reports, and see the status of badge applications. Because Authorized Signatories typically have other responsibilities within their company, any changes will need to be carefully considered and discussed to ensure that the personnel in the Signatory role are comfortable with the revised duties and responsibilities, and that their employers understand the potential impacts to workload.

Other stakeholders may not be directly involved with the IDMS but still have perspectives that should be considered. For example, construction companies and the airport departments responsible for construction can be negatively impacted by an inefficient badging process. Understanding the concerns and issues that these stakeholders may have with the existing process can provide guidance regarding changes that may be needed.

Other departments of the airport may be affected by changes to identity management processes that extend beyond credentialing. These include the airport IT and technical teams, whose participation will be required to implement and support the IDMS.

In summary, the more inclusive the engagement with stakeholders, the more likely it is that the selected IDMS will be efficient, effective, and representative of the needs of the stakeholder community.

3.8 Cost Considerations

Implementing an IDMS has cost considerations beyond the initial capital cost of the system. These can range widely depending on the type of system selected, the use of consultants and integrators, the state of existing IT infrastructure, and a number of other factors. The airport also needs to consider the operational and maintenance costs of the system over the working life of the IDMS.

Costs to consider may include, but are not limited to, the following elements:

- **Planning and Assessment Costs:** These may include the cost of project staff (permanent and temporary), staff support, and consultants, as well as other costs associated with planning for the project. This stage would focus on preparatory work such as collecting information, assessing the existing conditions, and developing an understanding and familiarity with IDMS and their capabilities.
- **Pre-procurement Costs:** Pre-procurement costs largely include staff and other labor resources. At this stage, the efforts would be focused on the development of procurement documents, interviews of vendors or contractors, and product demonstrations. It should be noted that the careful and detailed preparation of procurement documents—including operational and technical requirements, Service Level Agreement (SLA) requirements, maintenance requirements, and implementation requirements—is a wise investment.
- **Project Management Costs:** These include the costs of labor and associated items to manage the process of delivering the IDMS.
- **Capital Costs:** These include the direct costs for the IDMS, and may include associated costs such as improvements or expansion of IT and technology systems, upgrades to existing associated systems (e.g., the ACS), physical space improvements, permits, and other soft costs that may be borne by the vendor or contractor. This would include identifying and securing funding vehicles for the project.
- **Ongoing Operational Costs:** These include the costs of operating and maintaining the system throughout its operating life. Costs will typically be both internal and external. Internal costs may include staffing needed to support the IMDS after implementation, such as IT support or additional system operators or administrators. External costs are those associated with the integrator and/or IDMS manufacturer such as licensing fees, SLAs and maintenance support, training services, and potentially the cost of updates and upgrades.

3.9 Technical Requirements

One of the last steps in planning for an IDMS procurement is to establish a clear set of technical and/or performance requirements. These must adequately define the expected outcome and means of achieving that outcome so that a vendor can present an accurate bid or proposal and the airport can assess the suitability of the proposed solution.

The degree of detail in the technical requirements can range from a minimal set of desired outcomes to a fully developed set of technical requirements and measurable results. Based on the experiences of interviewed airports, there is not an approach that clearly results in a better end product. However, less specificity in requirements often leads to more costly proposals because vendors need to cover the risk of unknown requirements. The approach will depend on the airport's particular situation and preferred means of procurement and delivery.

When defining the technical requirements, the airport should consider the following:

- **Software systems and requirements:** These include the functional requirements for the IDMS software as well as operating systems, virtualization software and licensing, and any software upgrades or changes required to existing systems that will be tied to or affected by the introduction of the IDMS. This should include commercial and custom applications.
- **Requirements for data transfer from existing systems:** The airport should have a clear understanding of the scale and status of the dataset that will be transferred to the IDMS, including the location of the data, quality of the information, and the requirements associated with cleanup or corrective actions prior to or in conjunction with the IDMS implementation. The data may reside in disparate systems or may be duplicated in multiple systems. Understanding where data exists and which data sources will be used is important to ensuring a successful transfer of data.
- **Identification of integration and interface requirements:** This should include identifying all integrations and interfaces required or anticipated for the IDMS to function as envisioned. In developing this, the airport should consider the following:
    - Each integration and interface should be assessed to determine if it is necessary and how it is to be accomplished
    - The airport should understand that additional interfaces and integrations may be required and that some may be eliminated
    - The airport should be aware that the greater the number of integrations and interfaces required, the greater the risk of extended timelines and increased costs
- **Reporting systems and requirements:** The airport will need to define the types of reporting required and the methods to distribute the information. This may include electronic and hardcopy, as well as an information dashboard. As these reports may contain sensitive information, the airport should account for data security and integrity.
- **Data security and integrity:** Given the sensitivity of the information in an IDMS, a minimum set of requirements must be established to ensure the information is protected from both accidental and intentional release or access.
- **Auditing requirements:** Badging audits must be performed on a yearly basis, and the airport must identify the audit processes currently in use at the airport. The IDMS should support the audit functions in a manner that will meet the airport regulatory environment.
- **Computer workstations and associated equipment:** These should include quantities of equipment needed for the planned system. It is important to know the minimum technical specifications for the equipment and identify supporting software that must be installed on the workstations, particularly those that are not provided by the IDMS vendor. In addition, the age and condition of the current equipment should be considered to determine if it can to be reused or repurposed.

- **System redundancy requirements:** The expected system redundancy should be included in the technical requirements. In addition to redundancy, uptime metrics should be included based on the criticality of the IDMS and the downtime that would be considered acceptable. Redundancy could include separate physical servers, separate servers within a virtual server environment, or a cloud server. By defining the uptime metrics and stating whether high availability is required, the appropriate solution can be chosen and the associated costs included in the procurement.
- **Cloud-based vs. on-premises solution:** The airport must determine their preference for where the IDMS will reside (i.e., in local servers versus cloud servers). While there is a general trend in the technology industry to move to cloud-based solutions, there are concerns regarding the security of this approach, particularly given the types of data that are stored in the IDMS. Airport IT departments tend to favor the ability to closely monitor the information on premises over the potential to scale up storage space in the future on a cloud-based platform.

3.10 Operational and Process Requirements

In many cases, there are discrepancies between the way a process is documented and how it is actually performed. It is important to consider both when defining the processes that an IDMS will support. A proven approach is to involve credentialing office personnel in the documentation of existing process workflows and the creation of workflows using the IDMS. This will help uncover hidden processes and gaps in the documented processes, and capture improvements that have not been documented. To avoid getting bogged down in resolving discrepancies, it can be helpful to engage consultants who specialize in this kind of information development.

At a minimum, key processes to consider include the following:

- Company enrollment
- Authorized Signatory enrollment and training
- Badge application
- Interaction between badging office personnel and applicants
  - Identification verification
  - Fingerprinting
  - Adjudication of CHRC results and Rap Back notifications
  - Issuance of credentials
- SIDA and driver training (movement and non-movement area) – initial and recurring
- Badge renewal
- Lost badge replacement
- Badge revocation

AVOID OVER-CUSTOMIZATION

Avoid excessive customization of the IDMS. Certain customizations will be appropriate or essential, but the airport should find a balance between an off-the-shelf approach and a highly customized solution. Greater customization will require higher initial capital and ongoing operational costs.

Several airports noted issues related to the customization of their IDMS. One of the larger issues was that the customization was significant enough to effectively make the software a unique version. Because of this, the airport has not been able to update the software since its implementation. While upgrading the software may be possible, it would be a major effort. Airports stated that it would have been more prudent to adapt their processes to the off-the-shelf product whenever possible instead of customizing the product to their current process. These airports are now considering a complete replacement of their systems.

SECTION 4: IDMS PROCUREMENT

Several airports stated that their IDMS was procured as part of a larger project. In one case, the IDMS was part of a security-specific project that included access control and surveillance systems. The airport was able to use a best value procurement, allowing them to evaluate the bids received beyond the cost. However, as the procurement included access control and surveillance, the airport selected the winning proposal based on the overall offering, not just the IDMS. In another example, the IDMS was procured as part of a capital project that included the construction of a new concourse. This reduced the airport's ability to evaluate the IDMS product independently from the overall project, with the overall project being the primary selection. Unless the proposed IDMS was deemed to be non-compliant, the airport was bound to accept the IDMS selected by the prime contractor.

Overall, most airports noted that a dedicated procurement for an IDMS is the preferred method. This allows the airport to focus on the IDMS without also managing other competing priorities in a larger project. However, it is common for available funding to be restricted to larger programs, making procurement as part of a larger project the only option. In these situations, more detailed specifications may be required to ensure the IDMS meets the airport's needs.

The procurement methods detailed below could be utilized in both standalone and combined projects.

DESIGN-BID-BUILD

This is the traditional procurement method, with specifications provided that define the system, the expected features, and the expected integrations. A contractor, integrator, or manufacturer would provide a bid, and typically the lowest bid will be selected. This may vary depending upon the allowed procurement rules at the airport and restrictions based on the type of funding being used for the project. Choosing the winning proposal based on the lowest bid is generally not ideal for procurement of a software-based system. The lowest bid may not offer the level of customization needed to effectively manage the credentialing process. If possible, a best value selection is preferred.

DESIGN-BUILD

Some airports use a Design-Build method for IDMS procurement. While this is not a common approach for IT projects, it may be viable depending upon the airport's procurement rules. The Design-Build may start with a Construction Manager at Risk (CMAR) or an integrator that works with the airport to evaluate the products on the market and set the project budget and scope. The CMAR or integrator would procure the IDMS and oversee the implementation.

REQUEST FOR QUALIFICATIONS (RFQ)

Some airports indicated the use of an RFQ as part of IDMS procurement. The RFQ requests the airport-established minimum qualifications from the manufacturers or the integrator/manufacturer teams (if applicable), including the manufacturer's airport experience and airport references. Product demonstrations may also be required. The RFQ responses will be assessed and used to narrow down the manufacturers that will be invited to respond to the next phase of procurement. The next phase may be a bid, RFP, or best value procurement.

BID FOLLOWING RFQ

The bid of an IDMS after an RFQ is similar to the Design-Bid-Build format discussed above, but the respondents are pre-qualified to reduce the number of non-qualified bid submissions. The RFQ does not allow for exclusion of bidders based on whether the product aligns with the airport's needs, so this may not net the desired results. While the bidders are limited to a pre-qualified list, the airport would still be required to accept the lowest price bid that is deemed to be responsive.

REQUEST FOR PROPOSALS (RFP)

The RFP method allows manufacturers or manufacturer/integrator teams to submit proposals that the airport will evaluate using specific scoring criteria. While system cost is typically one of the scoring criteria, it is not the only factor. This method may allow the airport to include a product demonstration as part of the proposal evaluation. The RFP method allows the airport to consider other criteria instead of basing their selection strictly on the cost of the system. An RFP may follow an RFQ.

BEST VALUE

Best value includes more detailed specifications than the RFP method. However, the airport will be able to evaluate the proposal based on the proposer's qualifications as well as the product while using a scoring criteria similar to an RFP. This format is sometimes chosen when rules and regulations restrict the use of RFQ and RFP methods.

Most airports indicated that a best value method of procurement offered the most flexibility to choose the appropriate solution. This approach allows for including factors beyond cost of the solution, such as the experience of the system manufacturer in airports, a compliance matrix of required features, and a product demonstration. A best value procurement was recommended for airports of all sizes as permitted by the procurement rules and regulations that govern the airport.

4.1 Procurement Documents

It is recommended to establish a panel to assist in creating the procurement documents and evaluating the proposals received. The panel should represent the various entities within the airport that will utilize the IDMS. For example, a typical panel may include representatives from the credentialing office, airport security, IT, and the procurement office. A diverse panel brings multiple perspectives to evaluate all elements of the proposals.

While the main focus of this section is on the procurement of the IDMS, the procurement may include other related items. For example, the IDMS implementation may include the reconfiguration of the credentialing workstations or a complete renovation of the credentialing office to accommodate the updated workflows and processes. Regardless of the method of procurement, there are common elements that should be detailed in the procurement documents. These typically include:

EXISTING CONDITIONS

The existing conditions at the airport should be provided in the procurement document. For example, the number of active badge holders at the airport and any systems expected to be integrated with the IDMS (along with their current version) should be included. Any planned upgrades during the implementation should also be noted.

The current credentialing system (e.g., ACS, IDMS) should be provided, as this will inform the expected effort needed to transition the data between the existing system to the procured IDMS.

One lesson learned by the interviewed airports is to ensure the various systems to be integrated with the IDMS have been updated to the latest version. IDMS manufacturers generally only support the most current versions of software, and it is better to plan for updates prior to the system implementation rather than delay the project.

OBJECTIVES, GOALS, AND EXPECTED OUTCOMES

Procurement documents should detail the airport's expectations and system goals for the IDMS. Goals and expected outcomes may include the following:

- Paperless processes, including electronic submission and electronic signatures
- No re-entry of data between systems
- Automatic receipt of CHRC/STA results
- Management of the credentialing process, including automatic notification of badge status
- Integration of systems, such as ACS, CBT, DAC, PSIM/CAD
- Automatic report generation
- Simplification of audit process
- Facilitation of CBP eBadge process for Customs Seals
- Improvements in customer service metrics

CREDENTIALING WORKFLOW PROCESSES AND PROCEDURES

It is important for proposers to understand the processes and procedures that need to be included in the new IDMS. While baseline processes are included in federal regulations, most airports have unique requirements. These need to be clearly defined in the procurement documents to ensure they can be accommodated. However, airports also need to consider what can be changed in their current processes and procedures to match the products available on the market. This reduces the potential for errors in the system and challenges when upgrading to new versions.

SCOPE OF WORK

Procurement documents must clearly define the scope of work. The scope of work should include the system technical requirements as well as the roles and responsibilities of the IDMS provider, the airport, and any other relevant parties. See Section 4.3 for more details.

TESTING AND TRAINING

Procurement documents should clearly define the testing and training requirements and expectations. Many airports indicated that the testing and training provided by the vendor or integrator did not meet their expectations. Detailing these expectations upfront will help to ensure they are met.

Testing of the IDMS can be time consuming, and requires adequate support from the vendor or integrator. The functional requirements, as described in the procurement documents, should form the basis of system testing. The new IDMS should be tested against the requirements to demonstrate that the implemented system can perform the desired functions. The procurement document should define the expected testing program, the minimum testing time required, and the onsite support to be provided. For example, if the airport expects that testing will last two weeks and the manufacturer will have personnel onsite to perform and supervise the testing, then this should be stated in the procurement documents. Airports may also note if the manufacturer's personnel may work offsite with remote access to the system.

Training of the various user groups was identified as a major issue by multiple airports. Most airports expected training to be provided to credentialing operators, supervisors, and IT personnel supporting the system. However, the in-person training often fell short of the airports' expectations, with the testing phase often considered the training. The training was often a train-the-trainer format when the airport expected individual training for all of the system users. Additionally, airports expected training materials to be provided, such as manuals, videos, and other documentation. Many airports noted that they either did not receive any training materials or that they received some training materials, but they were generic and did not reflect the system as implemented at their airport.

To ensure that the training program meets the airport's expectations, the procurement documents should include requirements for the specific training requested, who will provide the training, what aspects of the IDMS the training will cover, the expected number of classes and attendees, the roles of the attendees, the duration expected, and if the trainer is required to be onsite for the training or if they can be remote. If training documents or user manuals are desired, then this should also be stated in the procurement document.

Lesson Learned: Training is critical. Training materials should be tailored to the project. Trainers should be conversant with the IDMS as configured for the airport.

ONGOING SUPPORT AND SERVICE LEVEL AGREEMENT (SLA) REQUIREMENTS

The procurement documents should clearly define the ongoing support and expected SLAs. Many airports stated that the level of ongoing support was not as expected, and that these requirements were not detailed in the procurement documents. Most IDMS will have associated ongoing costs, which typically include yearly licensing and support/maintenance costs. These costs are usually paid to the IDMS manufacturer and do not include any onsite support for the system. The most common type of support is contacting the manufacturer to resolve issues with the system. However, most of the support centers for the manufacturers are on a typical workday schedule, with select hours Monday through Friday. If airports require support to be provided after hours or on weekends, this should be clearly defined in the procurement document. SLAs usually focus on performance metrics that the manufacturer must meet when responding to support calls. However, if procurement documents do not require after-hours or weekend support, a callback within a preset time may not be enforceable.

If onsite support is desired, the airport may need to contract with an integrator. For example, if the airport needs assistance with the badging workstation peripherals, such as scanners, capture equipment, or badge printers, then this should be defined in the procurement documents, or a separate procurement for integrator services should be issued.

4.2 Vendor Evaluation and Selection

When responses to the procurement documents are received, the first step is to evaluate the submissions and confirm that the proposals are complete and contain all of the required elements. Submissions that are deemed acceptable can be further evaluated based on the submitted information. The procurement method will determine what may be considered for evaluation. Assuming that the procurement method is not the lowest bid option, the airport may weigh other factors, including:

VENDOR PRODUCT PERFORMANCE

The products offered should be reviewed and demonstrations should be required. The demonstrations will allow the airport to see the products, compare them, and determine which one most closely fits their requirements. The best product will offer the airport's desired features and meet their requirements for integrating with existing systems.

OVERALL AND INDIVIDUAL EXPERIENCE

The experience of the vendor and the integrator (if applicable) should be considered. Some vendors and integrators may have more experience or successful deployments overall, but others may have more experience with successful deployments at airports. Experience with airport IDMS implementation is essential, as an airport's environment and regulatory requirements are unique. In addition, the experience and certifications of the individuals proposed for the project implementation should be considered.

COST

While product performance and vendor experience are important, the cost of the IDMS must also be considered. The costs should include both initial costs and ongoing costs for the first five years of system ownership. Ongoing costs often include support, maintenance and licensing fees. Considering both the capital and operation/maintenance costs allows for comparison of the overall costs of the proposed system's lifetime. This will be especially important as different financial models are introduced to the market. For example, some vendors are starting to use a software-as-a-service model in which the initial costs may be low, but each transaction in the system will be billed as a cost, or each individual active in the system incurs a fee. While the cost may initially appear to be lower, these types of financial models may result in a significantly higher costs over the life of the system.

SYSTEM SUPPORT

System support during and after implementation is important to ensure a successful project. The airport will need to determine the level of support and nature of the support required from the manufacturer. Unless the airport is located in the same city as the IDMS manufacturer, the system support available will most likely be remote. Support for workstations and peripherals may need to be a separate contract with another entity, such as an integrator. If a particular vendor or manufacturer cannot offer the level of support and SLA required by the airport, or has a significant cost for providing the support, this should be considered during the vendor evaluation.

AIRPORT REFERENCES

It is recommended that the airport request references from existing airport clients currently operating the proposed system. It is recommended that the airport verify and collect any information from these references. The references should be considered as part of the overall selection process.

4.3 Scope of Work Development

One approach often used to define the scope of work is to provide a complete, technical-based scope. This type of scope provides detailed specifications of what needs to be included in the project, such as:

- Existing badging/IDMS software
- Current licensing agreements
- Quantity of IDMS workstations needed and locations
- Server redundancy and/or high availability requirements, including any test or development environments included in the implementation
- Peripherals to be provided by the proposers, including required quantities
- Existing IT infrastructure and infrastructure to be provided by the proposer
- Required integrations that lists specific systems to be integrated (including current version of each software) and the expected data to be exchanged between the systems
- List of current database fields
- Expected operation and process flows for the IDMS based on desired future airport operations
- Number of expected system users
- Number of badge holders
- Demarcation of expected work between the airport and the IDMS provider
- Project schedule or timeline
- Project testing and endurance requirements

The technical requirements should include all of the elements discussed in Section 3.9. While it is not necessary to define the exact data fields at this stage, it is important to outline the expected operation and interaction between the systems. In addition, the technical requirements should quantify the workstations and types to be provided as part of the project so that all hardware and licensing can be accounted for.

Another approach is to provide a performance and outcome-based scope of work. This type of scope provides details of the desired future state, but may not define the exact process flows or how the system is to be implemented. This type of procurement is more general and allows the system manufacturers to explain how their system and processes can meet the needs of the airport. This approach would typically include the following:

- Existing conditions
    - Existing workflows and processes
    - Existing infrastructure
    - Existing interfaces and integrations
- Roles and responsibilities of the airport and manufacturer and/or integrator
- Project objectives and outcomes
    - Minimum requirements for IDMS delivery
    - Desired project outcome
- Proposed schedule
- Proposed IDMS testing

The roles and responsibilities should be clearly delineated. For example, if the airport has an existing virtual server environment or storage array that is intended for use in the IDMS, the expected interaction between the system provider and the airport should be defined, including the expected lead times needed by the airport to meet the system provider’s schedule.

Both technical-based and outcome-based scopes of work should include all of the expected system implementations as noted in this section and as defined in Section 5.2. For example, if development and test environments are expected in addition to the production environment, then this should be clearly defined in the scope of work, to include the software, licenses, integrations, servers, and workstations required to support the additional environments.

Regardless of the scope type, it is recommended that a compliance matrix be included that lists the requirements set forth in the scope. It should be detailed enough to allow for clear and simple evaluation to determine if the IDMS provider meets the scope of work requirements. However, an overly long compliance matrix detailing every item will make the process for responding to the procurement time-consuming, not only for the proposers but also for the proposal evaluation and selection team.

The compliance matrix can also be used in system testing to assure the airport, through successful testing of the requirements, that the IDMS they requested is truly the system that is implemented.

4.4 Submittal and Documentation Requirements

Proposals should include sufficient detail to allow the airport to ensure that the proposer and the product meet the procurement requirements. To allow for an objective comparison, the submission requirements should be detailed in regard to content, expected page counts, and material to be included. A sample submission may include the following:

1. Cover page
2. Company background and experience
    a. Proposed product experience and history
    b. Integrator/implementer experience (if applicable)
3. Organizational structure of the company and any subcontractors
4. Required positions and staff resumes to fulfill those positions
    a. Project Manager
    b. Technical Lead
    c. Subject Matter Expert
    d. Database Administrator
    e. IT System Designer / IT Coodinator
    f. Installation staff
5. Proposer's understanding of the work
6. Compliance matrix for the proposed system
7. Project schedule
    a. Major milestones
    b. Coordination meetings and information gathering events
    c. Stakeholder meetings
8. Project quality management plan
9. Training plan
10. Warranty and support plan
11. Bid forms and other contractual elements
12. Appendixes as required for insurance, bonding, team certifications, etc.

In addition to the written proposal, many airports recommended that an onsite demonstration be performed by the system manufacturer. This allows the airport to determine if the base product will meet the airport's needs or if the solution will need a high level of customization. This demonstration can be mandatory for all proposers. However, many airports recommended performing a preliminary review of the proposal so that only the proposers deemed to be responsive are invited to demonstrate their product.

4.4.1 Project Quality Management

The proposal submission should include an overview of proposer's quality management approach that will be used to document the project. This may include a standard quality control manual, the proposer's change management process, and the approach to track all outstanding issues on the project.

Depending upon the size of the project, quality management may be part of the duties of the Project Manager, or may be a separate role on larger projects. It is up to the airport to determine whether this is considered a critical position that requires a dedicated person. If a separate position is desired for a specific project, the position should be added to the submission and a resume requested for this position.

4.4.2 Coordination Meetings

Coordination meetings will be important to meeting the project objectives. The proposals should provide a list of the expected and anticipated coordination meetings, the frequency of those meetings, and the stakeholders expected to attend. This will allow the airport to assess the impact on the existing staff as part of the proposal evaluation and selection process.

4.4.3 Stakeholder Engagement

Stakeholder engagement is important to successfully implement an IDMS. The IDMS provider should understand that stakeholders are an important part of the badging process. Proposers should indicate which stakeholders need to be involved, when they will need to be involved, and their expected level of participation in the overall project.

4.4.4 Warranty Requirements

A warranty should be included in the procurement requirements. The warranty period should start after final acceptance of the system and should cover at least one year. All costs associated with the system during this one-year period should be included in the procurement costs, including any licensing, support, and required on-site support.

After the warranty period, the support typically transitions to a support and maintenance agreement. It is recommended that the proposed support and maintenance details and costs (including upgrade costs) for the first three to five years be included in the procurement budget to allow for the airport to evaluate the total cost of ownership for the system.

4.5 Contract Considerations

The contract type used for the IDMS project should align with the airport's standard practices for procurement, but it is important to remember that an IDMS is a software system and not a brick-and-mortar construction. Contracts used for previous software procurement at the airport may provide guidance on the contract type and payment schedule that is appropriate for the IDMS.

Airports noted that a payment schedule based on project milestones was in line with other types of procurement, but manufacturers noted that overly specific payment schedules have occasionally resulted in payments not being issued in a timely manner. The payment schedule should accommodate the needs of the manufacturer and integrator (if applicable) to pay for the work performed, but should also protect the airport against non-conformance or other issues with the work. Balance is needed to create an equitable situation for all parties.

SECTION 5: IDMS IMPLEMENTATION

Implementation of an IDMS can be a lengthy and unpredictable process. Many airports noted that the implementation process often extended well beyond the initial implementation schedule. Lessons learned and factors to consider when working through the implementation process are included in the following sections.

5.1 Schedule and Key Milestones

The selected proposal should include a high level schedule outlining the manufacturer's implementation plan. After contracts are executed, the schedule should be reviewed with the airport's technical and management teams and finalized to include the key milestones, meetings, and deliverables. At a minimum, the schedule should include the following key milestones:

- **Planning:** The planning stage should include coordination of all workshops needed to gather data from the airport and its stakeholders and to map the process flows with the relevant parties.
- **Virtual Operation:** The virtual operation stage should include preparing a sample of the various workstation types, including all the peripherals and access to other features (such as a web portal). The intent is to allow the airport to fully test and work through the processes prior to the final migration to ensure that all the features are operating correctly. The virtual environment may be part of the Development and Test Environments if those are included in the procurement.
- **Migration:** Migration is the process of moving from the existing environment to the new IDMS, with all the associated integrations and data transfer. While this is often viewed as a single event, migration typically includes multiple tests before the final migration. For example, the migration of data from the existing system will likely be tested and reviewed multiple times, with any additional data grooming or correction performed between each test. Once the data is shown to cleanly transfer from the existing system to the IDMS and all integrations prove to be fully functional, the final migration can be scheduled.
- **System Testing:** System testing will be conducted in concert with the migration, and will continue after the migration to ensure everything is operating as expected. To allow for planning of resources, the schedule should reflect the level of testing required at each stage, the support required from the system manufacturer, the personnel required to be involved in each test, and the duration of each test.
- **Full Production and Operation:** The date of full production and operation should be clearly defined in the schedule.

The schedule should reflect all of the milestones and tests that need to be completed prior to full production and operation. In addition, a list of the resources required for all of the steps prior to full production and operation, as well as the expected support after this milestone, should be provided as part of this schedule.

Many of the interviewed airports reported having issues concerning their project schedule. In several cases, airports experienced significant schedule delays, ranging from several months to well over a year. There are always schedule risks in any complex project, including risks that can be directly controlled by the airport, contractor, or others, and those that are outside of direct control, such as supply chain delays.

An airport undertaking an IDMS project should work with the vendor to develop and manage the project schedule. Timeframes and durations should be informed by actual conditions and input from the vendor, consultants, contractors, and integrators, and should pay close attention to how the project will be managed at a working airport. Attention should also be paid to other projects, including physical building work and other technology projects, and how those may impact the availability of staff and stakeholders to engage and support the project. The schedule should be reviewed by the project team on an agreed-upon frequency and adjusted based on actual progress.

5.2 Environments

Three environments are recommended when implementing an IDMS: Test, Development, and Production. The multi-environment implementation will allow for testing of changes to the IDMS, and can also be used to test updates and upgrades to the other systems prior to going to Production.

The Test Environment should include test versions of the systems that will be integrated into the IDMS. At a minimum, this should include the ACS to ensure the transfer of data between the two systems. The airport should also consider using the test environment for any other systems that are integrated with the IDMS, such as the CBT, DAC, fingerprinting workstations, PSIM or CAD.

In addition to including the integrated systems in the Test Environment, many airports provided fully equipped workstations to allow personnel to test new features and train on the system. For example, a credentialing workstation may be provided with all the peripherals, including the camera for badge photos, scanner for identification documents, biometric capture device (if applicable), badge printer with encoder, and printer for reports. This will facilitate testing of all the typical functions at a workstation, including the printing of a badge that can be tested on readers in the ACS Test Environment. As a side benefit, the test workstation also can be used for training without impacting the IDMS Production Environment.

The Development Environment is used to test patches, hot fixes, and upgrades to verify the system's stability without impacting any other systems. This environment is typically designed specifically for use by the IDMS vendor and will not include any of the integrations.

The Production Environment is the live system in daily use at the airport. Systems are fully vetted and tested in the Development and Test Environments prior to implementation in the Production Environment. By the time a patch or software upgrade is implemented in the Production Environment, the airport should have fully tested the changes and have a high degree of confidence that all the possible issues with integration or data transfer have been identified and corrected.

5.3 Data Migration

The migration of data from the existing system to the new IDMS is one of the most important tasks associated with IDMS implementation. There are multiple aspects that make data migration difficult, time consuming, and labor-intensive.

Due to the sensitive nature of the data needed for credentialing, the handling of that data should be tightly controlled. If personnel outside of the airport will be allowed to access the data as part of the transition, appropriate controls should be established. The process for allowing access typically includes establishing agreements with the company and personnel that would access the data; establishing minimum cybersecurity control measures for the data while being transferred, tested, migrated, and stored; and determining who needs to access the data. The agreement should include the minimum requirements for encryption and control of the data, and require that all data be permanently erased by external entities once the migration is completed.

Data grooming is the process of auditing a database to remove old or redundant data and correct inaccurate data. The transition to a new system provides the opportunity to reduce the database size and remove the inactive users or companies, if such actions are compliant with the airport's data retention policy. Data grooming is usually the responsibility of the airport prior to the data cleanup phase, which is typically performed by the system manufacturer.

Data cleanup is the process of aligning the data with the format needed by the IDMS. For example, an IDMS will typically use pull-down menus for categories such as company name, but the company's name may not be entered consistently in the database (e.g., Southwest Airlines could be entered as SWA, Southwest, etc.). These should be made consistent to allow for a seamless transfer. Data consistency issues can often be addressed in the data transfer script, and are often the responsibility of the system manufacturer. However, this responsibility needs to be defined in the scope of work.

Data conflict resolution follows the data grooming and cleanup process. This addresses potential regulatory compliance issues with the data or other inconsistencies that may become evident as the data transfer is tested. For example, if the airport allows multiple badges for one individual, the data may appear to have duplicate records, but all records will be necessary to account for all the individual's badges in the IDMS (although the data may need to be reworked to meet the IDMS format). On the other hand, duplicate records that are not associated with multiple badges may need to be removed. Addressing these types of issues will likely be the responsibility of the airport.

5.4 Testing and Cutover

Once the data migration is complete and all the data issues have been resolved, the final implementation of the IDMS can begin. The test data will be fully populated in the IDMS and testing can be performed to ensure that the system is operating as required.

INTEGRATION TESTING

The integrations between the IDMS and the other systems must be tested. It is recommended to create a Test Environment and include all systems that will be integrated with the IDMS.

The most common systems integrated with the IDMS are the ACS, DAC, and CBT. If these are configured in a Test Environment, then testing the integrations will be fairly straightforward and can be performed without impacting the Production Environments for these systems. Integrating all the systems in the Test Environment will allow for full testing of the interfaces to ensure all required data is being exchanged without errors. Integration testing is a detailed process and takes a significant amount of time.

FUNCTIONAL USER ACCEPTANCE TESTING

Functional user acceptance testing does not begin until the test data has been populated in the Test Environment and the integrations (full or simulated) are operational. This testing encompasses all of the user functions, including the interfaces used by Authorized Signatories, Trusted Agents, and System Administrators. The testing should go through all the user interfaces and the interplay between the various user roles. For example, test scripts should be created for company management, Authorized Signatory creation and duties, the Trusted Agent duties, and the Administrative duties. The test scripts should run through all of the expected workflows and actions that will be needed to thoroughly test all the functions and identify any issues with the processes, input of data, or the data transfer.

CUTOVER

Once the Functional User Acceptance testing is completed, then it is time to transition into the Production Environment and cut over to full operation.

The timing of the cutover is critical. Most airports noted that it was done over a weekend, with the credentialing office closed on the Friday before and possibly the Monday after to provide adequate time for the cutover and required testing. All personnel will also need to complete training prior to the cutover. Training is discussed in Section 5.5.

The cutover process will make the IDMS the primary source of data for the ACS. Cards and associated access levels in the database may be updated as the data source is changed. In many cases, this will then cause the ACS to download the badge numbers and access rights to each field panel or device on the system. Depending upon the system architecture and the age of the equipment, the panel updates could be nearly instantaneous or could take a significant amount of time. Planning for the cutover should consider that the upload of data to the individual panels could restrict access through doors during the upload period. Cutover will also include the transition of the IDMS to the existing badging stations or, if new badging stations are being provided, the replacement of the existing badging stations.

Many airports planned to have some workstations switched over to the IDMS prior to the official cutover, allowing for the workstation operation to be confirmed in the Production Environment. This may be desirable if the airport has sufficient workstations available. Some airports noted that they set up new workstations with the associated peripherals at an alternate location and fully tested their operation on the IDMS before relocating them to the badging office. If a reconfiguration or relocation of the badging office is included in the overall project scope, the phasing of construction work should be coordinated with the pre- and post-cutover operations.

ROLL-BACK PLANNING

With any significant technology implementation, particularly those involving transfer of data and operation from an existing system to a new one, there is always a risk that the cutover to the new system may not go smoothly. Given the critical nature of airport security systems, and the credentialing and identity management systems in particular, it is essential to have a plan in place to roll back to the existing system.

While careful and thorough testing should identify any issues that could arise during the cutover, the systems used in a Test Environment are usually more limited than the systems that are eventually deployed and in use at the airport. For example, while the Test Environment ACS may have some field panels and readers connected, this often is a small number compared to the overall system. Issues may arise as the interfaces attempt to connect to the larger systems. If this occurs, it may be necessary to revert to the previous state of operation until the problems are resolved.

The strategy used to accommodate the roll-back will depend on the system architectures. If the systems have dedicated onsite servers, the most recent back-up (typically, performed immediately prior to the cutover) could be used to restore the system. If redundant servers are in use, one server may be held in reserve during the cutover and then promoted to the primary if the cutover is not successful. If the system is in an virtual environment, a new server instance could be created for the cutover and the existing servers kept in the virtualized environment until the cutover is complete. Regardless of the strategy chosen, all systems that will be impacted by the IDMS should be backed up or otherwise made ready for the cutover with the ability to go back to the pre-cutover state if needed.

The roll-back plan should establish a specific time that, should issues arise that have not been resolved, the systems will be rolled back and the cutover rescheduled. It is vital to pick a specific time and enforce it. Failure to do so could result in a failed cutover that impacts operations. The cutover can be rescheduled once the issues identified have been resolved and fully evaluated in the Test Environment.

SYSTEM AVAILABILITY TESTING

System Availability Testing is the process of tracking any errors in the system or integration. System Availability Testing, sometimes referred to as Endurance Testing, is intended to prove system stability and proper operation. This testing should begin at cutover and continue for a preset period (usually a minimum of 14 days).

A system log should be created to document any and all system issues, including a record of all system alerts, events, and equipment failures or problems, the date and time that the issue occurred or started, the person reporting the issue, and when and how the issue was resolved. At the end of the 14 days, the logs will be analyzed to determine if the system passed or failed.

Endurance and high availability metrics included in the procurement documents will be used during the System Availability Testing to prove that the system meets the airport's requirements. The pass/fail metrics should be determined prior to the test start. For example, if the IDMS experiences an unscheduled outage for longer than the predetermined limit, then the test would fail and need to be restarted.

SITE ACCEPTANCE TESTING

The purpose of Site Acceptance Testing is to prove that the system features and integrations are operating as expected, that the system provides the expected level of redundancy and fault tolerance, and that all data is being transferred accurately and without errors. The integrator and/or manufacturer will need to provide test scripts to check all system functions. The scripts should indicate the information to be input and the information to be received from other systems to verify that each function is fully operational. The test scripts should check reporting and auditing functions, badging and adjudication functions, and administrative functions. Site Acceptance Testing should also evaluate all of the possible IDMS failure scenarios and failover features to prove that the IDMS will remain operational and all integrations will be maintained. Site Acceptance Testing should continue until all of the test scripts are completed and all of the functions have passed.

5.5 Training

The expectations for training to be provided by the winning proposer should be clearly stated in the procurement documents. Airports will need to identify the populations that require training. Examples include:

- Trusted Agents / credentialing personnel
- Credentialing administrators
- System Administrators / IT personnel
- Authorized Signatories
- Additional user groups that may have access to the system for specific purposes, such as airport operations, airport security, and CBP

After identifying the various populations, it is important to consider the type of training required for each. The training could be an on-site, hands-on course led by a vendor-provided instructor, online training that is available to each user group, a training manual provided to each system user as a reference guide, or a train-the-trainer format. The airport should determine how many individuals from each population need to be trained to help determine the number of classes necessary. The airport should clearly define the training expectations in the procurement documents. It is also recommended that a requirement for recurring and refresher training be stated in the procurement documents. Consideration should also be given to the type of training materials provided by the manufacturer. Some airports prefer a hard copy or electronic document while others want a CBT module.

Many airports discussed requiring training personnel to be on-site for a minimum duration to ensure that the training is in line with the airport's expectations. For example, the procurement may require that the training personnel be onsite for not less than a specified number of days.

SCHEDULING AND TIMING OF TRAINING

The availability of the various populations should be considered. If six Trusted Agents or badging personnel require training, it is unlikely all of them will be available at the same time unless the training is completed on a weekend or holiday, or by shutting down the badging office during the training. The most common solution is to hold multiple classes. Authorized Signatory training often consists of multiple classes throughout the day to catch each work shift.

The timing of the training should also be considered. Many airports will perform the training several weeks prior to the planned system cutover to ensure that the training is completed on time. However, training on a system is not the same as working in the system, and operators often have more questions or require additional training after spending time in the system. Many airports noted that having additional training after cutover was useful to clarify the operation of the system.

REVIEW OF TRAINING MATERIALS AND APPROVAL OF TRAINING INSTRUCTORS

Many airports noted dissatisfaction with the training documents or training instructors. In order to ensure that the training will be as expected, it is recommended that airports require submission of instruction materials and instructor qualifications for review and approval prior to the first training.

The training material to be used for each population or user type should be submitted for review and approval no less than six weeks prior to the start of training. The training material should be fully reviewed by the airport, including comparing the materials against the Development and Test Environments to ensure that the materials are up to date. Several airports noted that the materials they received were for previous versions of the software, did not include any of the customizations provided for the system being installed, or were otherwise not adequate. By reviewing and approving the materials, the airport can ensure that the materials meet their expectations. If the materials are found to be inadequate, the cutover date can be postponed until the materials are updated or replaced.

Some airports also noted that the training instructors were not sufficiently knowledgeable or familiar with the system. In order to avoid this issue, airports recommended that the system provider be required to provide resumes or a list of relevant experience for each of the proposed instructors. If the instructor was just trained on the system or is not familiar with the specific system being provided for the airport, then the airport can reject the instructor or request additional information to verify that the instructor is qualified to provide the training.

5.6 Project Closeout

Once any required training, System Availability Testing, and System Acceptance Testing are complete, then the closeout of the project can begin. The closeout includes the receipt and review of all of the final system documentation, the start of the warranty period, and the transition from the implementation stage to the maintenance stage. The acceptance of the project will vary depending on the definition in the contract documents, with some contracts requiring completion of the project and others only defining beneficial use. It is recommended that the acceptance be tied to the receipt of all project documentation when possible, since receiving the documentation was noted as an issue by many airports. Holding the beginning of warranty and maintenance, as well as holding final payment, can provide leverage to ensure that these aspects of the project are not neglected.

Once the IDMS is fully accepted and in operation, the airport can decommission the legacy system and archive or destroy data in accordance with the airport's policies. If the previous system was an integral part of the ACS, such as a badging module, then it is likely that no decommissioning will be required. However, there may be data cleanup needed in the ACS database to remove data that now resides in the IDMS and is no longer needed in the ACS.

5.6.1 Maintenance

IDMS software will require maintenance and upgrades over the life of the system. This may be related to the proper operation of the system, but it may also be related to regulatory or operational changes.

The airport needs to maintain awareness of changes that can be anticipated, such as rules changes in the federal code, or software updates and patches. However, it is the vendor's responsibility to deliver these changes. Software updates and upgrades to the IDMS or integrated systems may impact the operation of the integrated systems. A plan should be developed to implement all software changes in a scheduled, controlled manner. All updates to the IDMS should be developed in the Development Environment and tested in the Test Environment prior to migration to the live system. This will help protect the IDMS from unexpected errors.

The maintenance contract should specifically address how upgrades and new features related to rule and regulatory changes will implemented, and how the associated costs will be handled. The airport may decide that these types of projects will be handled through change orders to the existing contract or by separate contracts. At the least, the contractual mechanism expected to be used should be included in the maintenance contract, as the scope of future upgrades is likely unknown at the time that the maintenance contract is executed. Considering these changes during the implementation or renewal phase of the Maintenance contract may help to provide some level of control over the future costs. For example, hourly rates for the various levels of support personnel can be included in the maintenance contract to set a baseline for labor costs.

When new features are brought forth, the airport will need to evaluate the features and determine the overall impact. This will include reviewing the processes and procedures that will be impacted and creating a scope of work for implementation to define expectations of the maintenance provider.

5.6.2 End-of-Life Considerations

At some point the IDMS will no longer be viable. This may be due to a scheduled termination of the product, decommissioning and/or replacement of associated systems that effectively render the IDMS non-functional, or various other reasons.

The airport should include the IDMS in their regular planning and assessment process, as well as any IT or security master or strategic planning. This should include being informed of the vendor's planned end of life for the IDMS and working this into the airport's planning, procurement, and budgeting with appropriate schedule allowances.

SECTION 6: SUMMARY OF BEST PRACTICES

The following is a summary of best practices based on input from airports.

ASSESS THE NEED

IDMS may be beneficial in many situations, but they are not always essential. Before engaging in a major effort to procure an IDMS, the airport should perform a needs assessment to determine if an IDMS is a suitable solution. The needs assessment may show that the investment is not necessary or practical under the current circumstances. This may be a matter of cost, complexity, or simply that the benefits are marginal and do not justify the effort.

DOCUMENT THE EXISTING CONDITIONS

Having a clear understanding of the existing systems, processes, procedures is essential to properly planning for a new IDMS. This baseline informs the path forward, outlines the level of effort required, and helps identify inefficiencies or issues in existing conditions. Knowing as many of the potential issues as possible before the procurement or implementation results in more effective delivery.

CONSIDER EXPERTS AND SUPPORT STAFF

For most airports, the procurement and implementation of an IDMS is an unfamiliar effort. Consultants with experience in the systems can be retained to advise and support airport staff. While this does incur additional cost, the advice and guidance provided may ultimately save money.

AVOID OVER-INTEGRATION

IDMS are designed to serve a particular set of functions in the airport environment. The airport should start with a clear understanding of their goals and requirements for the system, including justifications for each. Care should be taken to avoid making the system overly complex or introducing functions and integrations that do not provide a clear benefit.

AVOID OVER-CUSTOMIZATION

Avoid excessively customizing the IDMS solution. Certain customizations may be appropriate or essential, but the airport should balance between a simpler, off-the-shelf approach and something highly customized. Greater customization will require greater initial capital and ongoing operational costs to maintain. The airport should adapt their processes to the off-the-shelf product whenever possible instead of customizing the product to their current processes.

BEST VALUE PROCUREMENT

Most airports indicated that a best value method of procurement offered the most flexibility to choose the appropriate solution for their requirements. The main takeaway is to consider factors beyond the cost of the solutions, such as the system manufacturer’s experience in airports, a compliance matrix of required features, and a product demonstration.

DETERMINE PROPOSERS’ EXPERIENCE

Many airports noted that the proposers’ previous experience is an important factor to consider. Experience at airports should be given more weight than non-airport experience. Including this in the selection criteria is recommended.

REQUEST A COMPLIANCE MATRIX

A compliance matrix should be included in the procurement documents and subsequent proposals to verify that the proposed system can provide all the required elements. The matrix will allow the airport to evaluate and compare the submitted matrices and account for any non-compliant items.

CONDUCT A PRODUCT DEMONSTRATION

Numerous airports recommended including a product demonstration in the evaluation and selection process. While a system may provide the required features, understanding how the system functions will help evaluators determine if the base processes and flows fit the airport's needs, how closely the system matches the airport's processes, and how much the base processes will need to be customized.

DETERMINE TOTAL COST OF OWNERSHIP

Most airports recommended including the initial costs of the system implementation as well as at least five years of total costs in the procurement documents. By including the costs associated with licensing, support, and maintenance, the total cost of ownership can be more easily determined and compared between proposers. This approach will also enable airports to determine the funding that will be needed in the future.

ASSEMBLE A STAKEHOLDER PANEL

Establishing a panel to assist in creating the procurement documents and evaluating the proposals received is recommended. The panel should represent the various entities within the airport that will utilize the IDMS. A diverse panel brings multiple perspectives to evaluate all elements of the proposals.

DEVELOP A PROJECT SCHEDULE

An airport undertaking an IDMS project should work with the vendor to develop and manage the project schedule. Timeframes and durations should be informed by actual conditions and input from the vendor, consultants, contractors, and integrators, and should pay close attention to how the project will be managed at a working airport. Attention should also be paid to other projects, including physical building work and other technology projects, and how those may impact the availability of staff and stakeholders to engage and support the project. The schedule should be reviewed by the project team on an agreed-upon frequency and adjusted based on actual progress.

IMPLEMENT DEVELOPMENT, TEST, AND PRODUCTION ENVIRONMENTS

Three environments are recommended when implementing an IDMS: Test, Development and Production. The multi-environment implementation will not only allow for testing of changes to the IDMS, but it can also be used to test updates and upgrades to the other systems prior to going to Production.

PLAN FOR ROLL-BACK

With any significant technology implementation, particularly those involving a transfer of data and operation from an existing system to a new one, there is always a risk that the cutover to the new system may not go smoothly or may experience significant issues. Given the critical nature of airport security systems, and the credentialing and identity management systems in particular, it is essential to have a plan in place to roll back to the existing system.

REVIEW TRAINING DOCUMENTS

It is recommended that airports require submission of instruction materials and instructor qualifications for review and approval prior to the first training. Airports should carefully review the provided training to ensure it addresses the initial training of staff and users to familiarize them with the operations, use, and maintenance of the new IDMS, as well as training over the life of the system. Some airports also recommended requiring resumes or a list of relevant experience for the proposed instructors to ensure they meet the airport's expectations.

DEFINE PROJECT CLOSEOUT

The acceptance of the project will vary depending on the definition in the contract documents, with some contracts requiring completion of the project and others only defining beneficial use. When possible, it is recommended that the acceptance be tied to the receipt of all project documentation since receiving the documentation was noted as an issue by many airports. Holding the beginning of warranty and maintenance, as well as holding final payment, provides leverage to ensure that these aspects of the project are not neglected.

ADDRESS ONGOING MAINTENANCE

IDMS will require software maintenance and upgrades over the life of the system. These may be related to the proper operation of the system as well as to regulatory or operational changes that require changes to a system function or its configuration. The maintenance contract should specifically address how upgrades and new features related to rule and regulatory changes are implemented, and how the costs associated with those are handled.

PLAN FOR END OF LIFE

At some point the IDMS will no longer be a viable solution for the airport. As with any technology-based system, the airport should include the IDMS in their regular planning and assessment process, including any IT or security master or strategic planning. This should include being informed of the vendor's planned end of life for the IDMS, and working this into the airport's planning, procurement, and budgeting with appropriate schedule allowances.

SECTION 7: EMERGING TRENDS AND INNOVATION

The following emerging trends have been identified in the IDMS technology and operational domain for airports based on research and interviews conducted with the airports and IDMS vendors. Airports may consider these trends when determining their options and the path forward toward acquiring and implementing an IDMS.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Artificial Intelligence (AI) and Machine Learning (ML) are both growing areas in the technology community, particularly with regard to how systems may be optimized through consistent use. An example of this for IDMS that an AI/ML system can analyze patterns and assess information in the credentialing database to identify and predict the access requirements for individuals. The AI/ML identifies peer groups or individuals within a particular population, determines what their access rights are, and develops recommendations for new enrollees based on their peer group or use group.

In theory, the AI/ML model would reduce the level of effort for manual assignments and actions by establishing a set of rules based on past actions rather than based on policies or mandates. However, the AI/ML is also capable of learning incorrect patterns, so frequent audits of the system’s learned behaviors would be necessary to prevent inappropriate access assignments.

This approach is not currently applied to any of the commercial IDMS available to airports, though it is currently being developed and tested by a new provider.

SELF-SERVICE CAPABILITIES

IDMS self-service features are currently offered by only one known vendor at this time. It is possible that self-enrollment will become more commonplace and other self-service features will be added, such as the ability for a badge holder to change their PIN. Other capabilities might include getting status updates to their badge application.

However, this would only eliminate a brief period of interaction between credentialing staff and the individual applicant, limiting the benefits to be had from self-service capabilities.

BLOCKCHAIN

Blockchain is a system designed to record and secure information in databases using a combination of cryptographies, data blocks, and what is called a “distributed ledger.” The details of blockchain are too involved to be addressed in this guidebook, but they are growing in use in areas such as cryptocurrencies and financial services.

It is anticipated that blockchain may continue to grow in use, and it is worth careful consideration as a means to protect information in an environment such as IDMS. Currently, no major IDMS vendors offer blockchain as an option, and there is no clear indication as to when they may choose to do so.

For additional reading on blockchain, please refer to the National Institute of Standards and Technology article, *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. January 2020*, referenced in the bibliography.

IDMS AS A SERVICE

At present, commercially available IDMS solutions are provided to the airport and operated by designated airport staff. One future option may be for the IDMS services to be provided by a third party on a cost-per-transaction or cost-per-badge-holder payment model. The actual software and equipment would be owned, operated, and maintained by the third party. Based on discussions with vendors, this approach might require a modest upfront engineering or mobilization cost, but would otherwise involve limited capital expenses. The airport would charge badge holders for their badges and then pass on a portion of that payment to cover the IDMS service.

At present, no airports have been identified as using this approach, although some beta testing is being conducted. It is worth monitoring how well this solution works and whether it is adopted in the aviation sector.

CLOUD-BASED SOLUTIONS

Cloud-based solutions have been used in industries for many years and IDMS vendors either offer or plan to offer a cloud-based system. However, no interviewed airport uses this type of solution. Most concerns stem from the IT department’s concern for data security, ownership of the data once it is stored on the cloud, and the reliability of the connection from the cloud-based storage facility.

Cloud-based solutions may not be popular at airports yet, but they are being used for a growing number of applications in nearly every industry. It is worth being aware of the capability, the benefits, and the risks associated with the approach, and watching for improvements or actions taken in the vendor community to address concerns.

REFERENCES

Airport Security Magazine. “How to Overcome Airport Identity Management Challenges.” May 2018.

Aviation Security Advisory Committee. “Report of the Aviation Security Advisory Committee on Insider Threat at Airports.” Aviation Security Advisory Committee, July 19, 2018.

Department of Homeland Security. “Access Control Systems.” Code of Federal Regulations, Title 49 (2010): 333-334.

Department of Homeland Security. “Identification Systems.” Code of Federal Regulations, Title 49 (2010): 338-339.

Department of Homeland Security. “Security of the Secured Area.” Code of Federal Regulations, Title 49 (2010): 332.

Department of Homeland Security. “Security of the Air Operations Area (AOA).” Code of Federal Regulations, Title 49 (2010): 327-328.

Department of Homeland Security. “Security of the Security Identification Display Area (SIDA).” Code of Federal Regulations, Title 49 (2010): 333.

Department of Homeland Security Office of Inspector General. “Transportation Security Administration’s Controls over SIDA Badges, Uniforms, and Identification Cards,” OIG-08-92 (September 2008).

Department of Homeland Security Office of Inspector General. “TSA Could Improve Its Oversight of Airport Controls over Access Media Badges,” OIG-17-04 (October 2016).

Garcia, Mary Lynn. 2008. The Design and Evaluation of Physical Protection Systems - 2nd Edition. Amsterdam: Elsevier/Butterworth-Heinemann.

HID Global Corporation/ASSA ABBLOY AB, “A Holistic Approach to Identity and Authentication,” (2018).

Grassi, Paul, Digital Identity Guidelines: Enrollment and Identity Proofing, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63A, (June 2017).

Hu, Vincent, Verification and Test Methods for Access Control Policies/Models, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-192 (June 2017).

IATA, “Aviation Identification & Authorization System,” (August 2015).

McCarthy, Jim, Identity and Access Management for Electric Utilities, National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-2 (July 2018).

National Institute of Standards and Technology, “A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems.” (January, 2020).

National Safe Skies Alliance, Inc., Program for Applied Research in Airport Security PARAS 0020, “Strategies for Effective Airport Identification Media Accountability and Control.” (December 2019).

National Safe Skies Alliance, Inc., Program for Applied Research in Airport Security PARAS 028, “Recommended Security Guidelines for Airport Planning, Design and Construction.” (February 2021).

National Safe Skies Alliance, Inc., Program for Applied Research in Airport Security PARAS 0029, “Update PARAS 0001 Criminal History Record Checks (CHRCs) and Vetting Aviation Workers.” (October 2020).

National Safe Skies Alliance, Inc., Program for Applied Research in Airport Security PARAS 0030, “Guidance for Access Control System Transitions.” (August 2021).

RTCA, “Standards for Airport Access Control Systems,” DO-230K (June 2021).

Sennewald, Charles A. 2003. Effective Security Management - 4th Edition . Oxford: Elsevier/ Butterworth Heinemann.

Smart Card Alliance, “The Commercial Identity Verification (CIV) Credential – Leveraging FIPS 201 and the PIV Specifications: Is the CIV Credential Right for You?” (October 2011).

ASAC Report of the Aviation Security Advisory Committee on Insider Threats at Airports, July 19th, 2018.

IATA Aviation Identification & Authorization System, Aug 2015.

Smart Card Alliance: The Commercial Identity Verification (CIV) Credential – Leveraging FIPS 201 and the PIV Specifications: Is the CIV Credential Right for You?, Oct 2011.

HID A Holistic Approach To Identity And Authentication.

Security Magazine: How to Overcome Airport Identity Management Challenges, May 2018.

APPENDIX A: INTERVIEW PARTICIPANTS

Interviews were conducted with the following airports, DAC Service Providers, and IDMS solution or service providers.

AIRPORTS

- Hartsfield–Jackson Atlanta International Airport
  - Keith Jackson – Assistant Director of Safety and Security
  - Tanna Almond – Airport Security Manager, Credentialing
- Baltimore/Washington International Thurgood Marshall Airport
  - Robert Boblitz – Director for Airport Security
  - Aliesha Gomez – Supervisor of Badge Training
  - Nathaniel Tubman – Assistant Manager of Airport Security
  - Rick Thorne – Manager of Airport Security
- Boston Logan International Airport
  - Antonella de Filippis, ACE – Manager Aviation Security, Credentialing and Violations; Liaison to the Joint Terrorism Task Force; Alt Airport Security Coordinator
  - Nancy Pullen – Senior IT Project Manager
- Dallas Fort Worth International Airport
  - Mike Wahl – Senior Manager, ITS Control Systems
- Friedman Memorial Airport
  - Steve Guthrie – Airport Security Manager
- Oakland International Airport
  - Jacob Graef – Aviation Security Superintendent
  - Doug Mansel – Manager, Aviation Security
- Seattle Tacoma International Airport
  - Lauren Curtis – Senior Manager Credentialing and Access Aviation Security
- San Antonio International Airport
  - Chris Cole – Airport Security Manager
  - Yvette Santos – Airport Coordinator in Badging
- San Francisco International Airport
  - Abedoon Jamal – Security Access Office Services Manager, Safety & Security
- Tampa International Airport
  - Mary Ouimet – Airport Credentialing Manager

DESIGNATED AVIATION CHANNELING SERVICE PROVIDERS

- American Association of Airport Executives (AAAE)
  - Sarah Pilli – Vice President AAAE Services,
- Telos Identity Management Solutions, LLC
  - Dawn Lucini – Vice President Aviation Security

COMPUTER-BASED TRAINING PROVIDERS

- American Association of Airport Executives
  - Kyle Herbig – Vice President Customer Solutions

INDUSTRY

Vendors

- AlertEnterprise, Inc.
  - Imran Rana – Sr. Vice President
- Genetec Inc.
  - Joe Degrassi – Director of Sales
  - David Lenot – Global Critical Infrastructure Practice lead
- HID Global
  - Russell Compton – Director of Aviation at HID Global
- Honeywell
  - Mike Trilk – Sr. Vertical Account Manager, Transportation
  - Chris Cola – Software Engineer Principal
- Intellisoft
  - David Peeples – CEO
- Vector Flow
  - Vik Ghai – Chief Technology Officer

Integrators

- Convergint
  - Matt Powell – Principal, Transportation Markets
- MC Dean
  - Calin Andronescu – Network Engineer

APPENDIX B: INTERVIEW QUESTIONS

This appendix provides the lists of interview questions used for each of the four interview groups that participated in the collection of data.

AIRPORT AND STAKEHOLDER FOCUS GROUP QUESTIONNAIRE

Category/Element/Question
Category 1 – General
Element 1.1 – Participants
1.1.1 Name /current title/ years experience - airport badging
1.1.2 Role in regard to badging at the airport
1.1.3 IDMS - Currently utilize or future plans to implement?
Element 1.2 – Badging
1.2.1 Badged population size 1.2.1.1 Pre-covid, lowest level, post-covid
1.2.2 Trusted Agents 1.2.2.1 Total employed 1.2.2.2 Average daily on-duty
1.2.3 Badging Office Layout 1.2.3.1 Number of stations
1.2.4 Remote & Local Capabilities 1.2.4.1 CBT or other services administered remotely? 1.2.4.2 Office accessible from typical applicant work area?
1.2.5 Badging process summary 1.2.5.1 Badging forms 1.2.5.2 ID scans 1.2.5.3 Approval Process 1.2.5.4 Notifications 1.2.5.5 Appointment Scheduling
Element 1.3 – Needs Assessment
1.3.1 IDMS considerations 1.3.1.1 Organizational/procedural challenges driving IDMS consideration 1.3.1.2 Business Process Improvements desired
1.3.2 Needs Assessment 1.3.2.1 Performed prior to procurement? 1.3.2.2 Level of stakeholder engagement
1.3.3 IDMS Cost Justification / Rationalization 1.3.3.1 ROI / TCO / other metrics utilized
Element 1.4 – Planning
1.4.1 RFP / Requirements 1.4.1.1 Strategies for list of IDMS requirements?

Category/Element/Question
1.4.2 Existing Policies and Procedures
1.4.2.1 Evaluated prior to IDMS considerations
1.4.2.2 Used as baseline for IDMS business requirements?
1.4.2.3 Data / Process flowcharts developed?
1.4.3 External SME / consultant utilized
1.4.4 Stakeholders
1.4.4.1 Breadth of stakeholders consulted?
1.4.4.2 Badging Office/Business / Construction / Procurement/Purchasing / Airport Security / DOA Airside/Landside / Local Police / CBP/TSA / Financial / Real Estate
1.4.5 Front Line worker involved?
1.4.5.1 Badging Office Staff
1.4.5.2 TAs
1.4.6 System Requirements
1.4.6.1 Requirements Matrix utilized to compile and reconcile stakeholder requests prior to contractual documentation development?
1.4.7 Stakeholder engagement effectiveness
1.4.7.1 Management and / or individual contributors engaged?
1.4.7.2 In person, phone, email conversations?
1.4.7.3 Were stakeholders allowed to review other department requests to uncover procedural inconsistencies?
Category 2– Procurement Processes
Element 2.1 – Purchasing
2.1.1 Contract vehicle type
2.1.1.1 RFP, RFQ, RFI, on-call contract, etc.
2.1.1.2 External consultant / SME utilized
2.1.1.3 Possible to share?
2.1.2 Documentation Development
2.1.2.1 Stakeholders included:
2.1.2.2 Airport Security/Badging Operations, IT, Senior management, Vendor, Integrator?
2.1.3 Project Schedule
2.1.3.1 Included in purchasing docs?
2.1.3.2 Milestone schedules included in RFP?
2.1.4 Solicitation response evaluation
2.1.4.1 Standard set of evaluation criteria utilized?
2.1.4.2 Compliance matrix utilized?
Category 3 – Implementation
Element 3.1 – Implementation
3.1.1 Project Management
3.1.1.1 PM duties handled internally, or external resources utilized
3.1.2 Implementation Plan
3.1.2.1 Cut-over plan included?
3.1.3 How closely did the team track with the plan?
3.1.4 Acceptance Process

Category/Element/Question
3.1.4.1 Project Deliverable Criteria for airport acceptance well-defined and followed? 3.1.5 Deliverables match requirements set forth within the RFP?
3.1.6 Architecture 3.1.6.1 Data Migration Issues 3.1.6.2 Non-COTS functionality and customizations 3.1.7 Hosted in-house, virtually, cloud based, etc.
3.1.8 Integrations 3.1.8.1 Number of systems integrated 3.1.8.2 Detail systems integrated, examples below 3.1.9 Access control, parking, badging, timekeeping, CBT/TSA/Local police, reporting and auditing software
3.1.10 Training 3.1.10.1 What departments received training and levels included 3.1.10.2 Training provided was sufficient for the airport's needs? 3.1.11 Manuals and documentation were sufficient?
3.1.12 Go-Live 3.1.13 Describe operational support from vendor, in-house, External SMEs and/or consultants
Category 4 – Current IDMS Process / Lessons Learned
Element 4.1 – Current IDMS Process
4.1.1 General Description 4.1.1.1 Describe how the system is utilized within the airport 4.1.1.2 How does the IDMS facilitate inter-departmental processes
4.1.2 Change Management Plan 4.1.2.1 Including interdepartmental communication processes
4.1.3 Badging Office 4.1.3.1 Operational changes identified, defined and documented 4.1.3.2 Changes to operational trainings required?
Element 4.2 – Lessons Learned
4.2.1 Project Management 4.2.1.1 Budgetary concerns / project finished on budget 4.2.1.2 Unexpected costs and /or paint points 4.2.1.3 Delays, procurement problems, lead-time issues
4.2.2 Scheduling 4.2.2.1 Contractor provided schedules were reasonable, accurate, and followed accordingly?
4.2.3 Interfaces 4.2.3.1 Integration issues, cumbersome or unexpected challenges 4.2.3.2 Positive experiences
Category 5 – Ongoing Considerations and Replacement Planning
Element 5.1 – Maintenance and Resiliency
5.1.1 Ongoing Support 5.1.1.1 Describe operational support contracts 5.1.1.2 Support provided from Manufacturer, Vendor or external professional services
5.1.2 Expected System Lifecycle

Category/Element/Question
Element 5.2 – Future-Proofing, Refreshing and Replacement
5.2.1 End of life consideration
5.2.1.1 Plans to refresh or replace the current IDMS
Open Dialogue: Please take this opportunity to freely discuss any items not included in the questionnaire:
1.
2.
3.

INTEGRATOR FOCUS GROUP QUESTIONNAIRE

Category/Element/Question	
Category 1 – General	
Element 1.1 – Participants	
1.1.1	Name /current title/ years experience with providing Integration services
1.1.2	Role in regard to implementing IDMS at airports
1.1.3	Years experience working with IDMS? Airports worked with to implement IDMS?
Element 1.2 – Integrator Information	
1.2.1	Integrator Name
1.2.2	Integrator Background, size (offices, employee counts, etc.)
1.2.3	General overview of Integrator experience with IDMS, airports implemented, etc.
Element 1.3 – Planning	
1.3.1	Which IDMS systems / manufacturers have you implemented?
1.3.1	Please describe a few of the implementations performed including airport, integrations, and general description including workstations, badge printers, other users, and badging population.
Element 1.4 - Planning	
1.4.1	Was the Integrator involved in the planning of the system?
1.4.2	If involved, did the integrator document the existing policies and procedures?
1.4.3	Did the Integrator evaluate policies and procedures prior to proposing an IDMS??
1.4.4	Were the policies and procedures used to form the baseline IDMS business rule requirements?
1.4.5	Were the IDMS data and process flowcharts provided as part of procurement or developed as part of the IDMS implementation? If provided, were significant revisions needed?
1.4.6	Was an external SME / Consultant included in the project? If so, what was the scope of work or focus area defined for the SME / Consultant?
1.4.7	Please discuss the Stakeholders involved in the Planning process?
Category 2– Procurement Processes	
Element 2.1 – Procurement	
2.1.1	How were the IDMS systems procured? Please note the contractor vehicles used (RFQ, RFP, Bid, on-call contract, etc.)
2.1.2	Please note the Solicitation Response and the evaluation.
2.1.3	Did the procurements utilize a standard set of solicitation requirements?
2.1.4	Were compliance matrixes included as part of the solicitation responses?
2.1.5	Are project schedules typically included in the procurement documentation? If so, were the schedules realistic?
2.1.6	What type of contracts are typically used for this type of project? Low bid, CMAR, lump sum, etc.
Category 3 – Implementation	
Element 3.1 – Implementation	
3.1.1	Please discuss the Project Management for the IDMS. Did the airport provide a PM, or was it outsourced?
3.1.2	Was an implementation plan including a cut-over plan provided for the project or does the integrator typically provide?
3.1.3	Does the integrator typically define the testing and acceptance criteria for project, or was it driven by the

Category/Element/Question	
	airport? Please describe the Airport system acceptance process.
3.1.4	Please discuss implementation issues that have arisen on IDMS projects including items such as data migration issues, customizations required, or testing and training delays.
3.1.5	Please discuss the level of training provided as part of the IDMS. Are training materials typically provided by the vendor/manufacturer or created by the integrator?
3.1.6	What support was provided during the go-live portion of the project?
3.1.7	Please note the operational support requested by the airport from the integrator.
3.1.8	Did the overall deliverables match what was defined in the project scope? Please elaborate on items that were not included or included but not necessary.
3.1.9	Please discuss the typical system installation from a headend perspective and what trends you are seeing. Are headends typically implemented on dedicated server environments, virtualized environments, in the cloud, or a hybrid? What do you foresee as the future typical installation?
3.1.10	What levels of redundancy are typically included in the implementation?
3.1.11	Describe any operational changes that took place as part of the implementation. Did the airport expect these changes? How were the changes identified, defined, and documented? Were changes included as part of the training?
Category 4 –Maintenance and Support, Future Proofing, Refreshing, and Replacement	
Element 4.1 – Maintenance and Support, Future Proofing, Refreshing, and Replacement	
4.1.1	What on-going Maintenance and Support was requested by the airport going forward? Please note what was supported by the airport versus the integrator or the manufacturer.
4.1.2	Please describe the typical ongoing cost items including on-going license costs, support costs, on-site maintenance support, and SLA agreements typically included.
4.1.3	What is the expected life-cycle of the system? Please discuss upgrades, replacement/refresh of hardware, and any planning related to system replacement.
4.1.4	Please discuss Change Management processes that are typically implemented as part of an IDMS.
Category 5 – Lessons Learned and Value Added	
Element 5.1 – Lessons Learned	
5.1.1	Please describe any lessons learned while implementing an IDMS from the Integrator side
Element 5.2 –Integrator Value Added	
5.2.1	Please discuss the value added by the use of an Integrator versus an airport contracting directly with an IDMS manufacturer for an IDMS implementation.
Open Dialogue: Please take this opportunity to freely discuss any items not included in the questionnaire:	
1.	
2.	
3.	

MANUFACTURER FOCUS GROUP QUESTIONNAIRE

Category/Element/Question	
Category 1 – General	
Element 1.1 – Participants	
1.1.1	Name /current title/ years experience with providing IDMS Systems for airports
1.1.2	Role in regard to implementing IDMS at airports
1.1.3	Years experience working with IDMS? Airports worked with to implement IDMS?
Element 1.2 – Integrator Information	
1.2.1	Manufacturer Name
1.2.2	Manufacturer Background, size (office(s), locations, employee counts, etc.)
1.2.3	General overview of experience with IDMS at airports, quantity implemented, etc.
Element 1.3 – Planning	
1.3.1	Which Access Control systems / manufacturers have you implemented IDMS with?
1.3.1	Please describe the top three implementations performed including airport, integrations, and general description including workstations, badge printers, other users, and badging population.
Element 1.4 - Planning	
1.4.1	Do you prefer to have an integrator involved in the implementations or not? If so, which integrators have you worked with?
1.4.2	Does the implementation typically document the existing policies and procedures? What is the process for integrating the process, policies, and procedures with the IDMS?
1.4.3	How are policies and procedures evaluated prior to proposing to provide an IDMS??
1.4.4	Were the policies and procedures used to form the baseline IDMS implementation?
1.4.5	Are the IDMS data and process flowcharts typically provided as part of procurement or developed as part of the IDMS implementation? If provided, were significant revisions needed?
1.4.6	Is an external SME / Consultant typically included in the project? If so, what was the scope of work or focus area defined for the SME / Consultant?
1.4.7	Please discuss the typical Airport Stakeholders involved in the Planning process?
Category 2– Procurement Processes	
Element 2.1 – Procurement	
2.1.1	How were the IDMS systems procured? Please note the contractor vehicles used (RFQ, RFP, Bid, on-call contract, etc.)
2.1.2	Please note the Solicitation Response and the evaluation.
2.1.3	Did the procurements utilize a standard set of solicitation requirements?
2.1.4	Are compliance matrixes typically included as part of the solicitation responses?
2.1.5	Are project schedules typically included in the procurement documentation? If so, are the schedules realistic?
2.1.6	What type of contracts are typically used for this type of project? Low bid, lump sum, best value, etc.
Category 3 – Implementation	
Element 3.1 – Implementation	
3.1.1	Please discuss the Project Management for the IDMS. Did the airport provide a PM, or was it outsourced?
3.1.2	Was an implementation plan including a cut-over plan provided for the project or does the manufacturer

Category/Element/Question	
	typically provide?
3.1.3	Does the manufacturer typically define the testing and acceptance criteria for project, or was it driven by the airport? Please describe the system acceptance process.
3.1.4	Please discuss implementation issues that have arisen on IDMS projects including items such as data migration issues, customizations required, or testing and training delays.
3.1.5	Please discuss the level of training provided as part of the IDMS. Are training materials typically provided? Training Videos? Or is it customized in-person training?
3.1.6	What support was provided during the go-live portion of the project?
3.1.7	Please discuss the operational support requested by the airport.
3.1.8	Did the overall deliverables match what was defined in the project scope? Please elaborate on items that were not included or included but not necessary.
3.1.9	Please discuss the typical system installation from a headend perspective and what trends you are seeing. Are headends typically implemented on dedicated server environments, virtualized environments, in the cloud, or a hybrid? What do you foresee as the future typical installation?
3.1.10	What levels of redundancy are typically included in the implementation?
3.1.11	Describe any operational changes that took place as part of the implementation. Did the airport expect these changes? How were the changes identified, defined, and documented? Were changes included as part of the training?
Category 4 –Maintenance and Support, Future Proofing, Refreshing, and Replacement	
Element 4.1 – Maintenance and Support, Future Proofing, Refreshing, and Replacement	
4.1.1	What on-going Maintenance and Support was requested by the airport going forward? Please note what is typically supported by the airport versus an integrator (if applicable) versus the manufacturer.
4.1.2	Please describe the typical ongoing cost items including on-going license costs, support costs, on-site maintenance support, and SLA agreements typically included.
4.1.3	What is the expected life-cycle of the system? Please discuss upgrades, replacement/refresh of hardware, and any planning related to system replacement.
4.1.4	Please discuss Change Management processes that are typically implemented as part of an IDMS.
Category 5 – Lessons Learned and Value Added	
Element 5.1 – Lessons Learned	
5.1.1	Please describe any lessons learned while implementing an IDMS from the manufacturer side
Element 5.2 –Integrator Value Added	
5.2.1	Please discuss the value added by the use of an Integrator versus an airport contracting directly with an IDMS manufacturer for an IDMS implementation.
Open Dialogue: Please take this opportunity to freely discuss any items not included in the questionnaire:	
1.	
2.	
3.	

DAC FOCUS GROUP QUESTIONNAIRE

Category/Element/Question	
Category 1 – General	
Element 1.1 – Participants	
1.1.1	Name /current title/ years experience with providing DAC services
1.1.2	Role in regard to DAC services
1.1.3	Current quantity of airports currently using this DAC for STA/CHRC and Rap Back services
Element 1.2 – IDMS Systems	
1.2.1	Which IDMS vendors/systems are you currently working with?
1.2.2	Describe the integration provided between you and the various IDMS platforms for submission and receipt of results.
1.2.3	How do the services provided to airports with IDMS differ from services for airports without IDMS?
Element 1.3 – Planning	
1.3.1	What planning is typically required from the DAC to implement an IDMS at an airport?
1.3.2	How does the planning vary depending upon the use of an IDMS versus airports without an IDMS?
1.3.3	Are there cost differences from the DAC side to implement an IDMS versus not having an IDMS?
1.3.4	Are there any additional pitfalls that need to be considered associated with using an IDMS?
1.3.5	Are there any regulatory differences from the DAC side affecting airports with an IDMS versus not having an IDMS?
Category 2– Procurement Processes	
Element 2.1 – Purchasing	
2.1.1	Does the overall procurement of DAC services vary if an IDMS is to be implemented? Please describe.
Category 3 – Implementation	
Element 3.1 – Implementation	
3.1.1	Does the use of an IDMS impact the implementation of DAC services?
3.1.2	In your experience, do IDMS systems make the interface with the DAC more difficult or easier?
3.1.3	Does the DAC provide integrations to IDMS products? If so, which.
3.1.4	Discuss the benefits/drawbacks of data scrubbing/migration with/without an IDMS
3.1.5	How do new SD's affect the implementation of an IDMS interfaced to the DAC?
3.1.6	Please note the systems currently integrated or interfaced with your DAC.
Category 4 – Current IDMS Process / Lessons Learned	
Element 4.1 – Current IDMS/DAC Process	
4.1.1	Does the use of an IDMS impact the workflow in regard to the DAC?
4.1.2	Do you provide different information to an airport with an IDMS than to one without an IDMS? If so, please describe.
Element 4.2 – Lessons Learned	
4.2.1	Please describe any lessons learned while implementing an IDMS from the DAC side.
4.2.2	Are the costs associated with DAC services the same with IDMS as without an IDMS?

Category/Element/Question
Category 5 – Ongoing Considerations and Replacement Planning
Element 5.1 – Maintenance and Resiliency
5.1.1 Any ongoing considerations from the DAC side in regard to ongoing maintenance and support?
Element 5.2 – Future-Proofing, Refreshing and Replacement
5.2.1 Any upcoming advancements in regard to DAC services that airports and IDMS vendors should be aware of?
Open Dialogue: Please take this opportunity to freely discuss any items not included in the questionnaire:
1.
2.
3.