



PARAS

PROGRAM FOR APPLIED
RESEARCH IN AIRPORT SECURITY



PARAS 0020

December 2019

Strategies for Effective Airport Identification Media Accountability and Control

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Anne Marie Pellerin
Sean Cusson
LAM LHA
Alexandria, VA

Donald Zoufal
Crowznest Consulting
Chicago, IL

Mark Crosby
Ross & Baruzzini
St. Louis, MO

Michael Keegan
Milwaukee, WI

© 2019 National Safe Skies Alliance, Inc. All rights reserved.

COPYRIGHT INFORMATION

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

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

NOTICE

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

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

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

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

NATIONAL SAFE SKIES ALLIANCE, INC.

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

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

Through PARAS (Program for Appplied 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 Special Programs Manager*

PARAS 0020 PROJECT PANEL

Jordan Christensen *Boise Airport*

Colleen Chamberlain *American Association of Airport Executives*

Lauren Curtis *Port of Seattle*

Antonella Defilippis *Massachusetts Port Authority*

Dawn Lucini *Telos Identity Management Solutions*

Jeremy Worrall *State of Alaska DOT*

AUTHOR ACKNOWLEDGMENTS

The Project Team would like to express our sincere gratitude to the airport operators that took the time to speak with us about their ID media programs. Without their time and willingness to discuss their programs in detail, we would not have been able to conduct such an in-depth review.

We would also like to thank Ilana Lisann and Lauren Peterson for their efforts in conducting research for the project.

CONTENTS

EXECUTIVE SUMMARY	iii
PARAS ACRONYMS	vii
ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS	viii
SECTION 1: INTRODUCTION	1
1.1 Overview	1
1.2 Challenges Affecting ID Media Accountability and Control	1
1.3 Research Approach	2
1.4 Document Layout	3
SECTION 2: REGULATORY HISTORY	4
2.1 Automated Access Control, Human Factors, and ID Media Issuance	4
2.2 Managing and Auditing Unescorted Access Identification System	4
2.3 Better Accounting and TSA Oversight	5
2.4 Planning for the Future	6
SECTION 3: ID MEDIA PROGRAM	7
3.1 ID Media Program Balance	7
3.2 Successful ID Media Program Commonalities	8
SECTION 4: ID MEDIA ISSUANCE	10
4.1 Key ID Media Issuance Considerations	10
4.2 Potential ID Media Issuance Issues	10
4.3 ID Media Issues Processes, Procedures, and Strategies to Consider	10
4.3.1 Standard ID Media Application	11
4.3.2 ID Media Applicant Responsibility Sheet	12
4.3.3 One ID Media	13
4.3.4 ID Media Expiration Periods	14
SECTION 5: TRAINING	19
5.1 Overview of Training	19
5.2 Key Training Considerations	20
5.3 Potential Training Issues	21
5.4 Training Processes, Procedures, and Strategies to Consider	21
5.4.1 New Badge Holder Training	21
5.4.2 Recurrent Training	22
5.4.3 Peer-to-Peer Authorized Signatory Training	24
5.4.4 Quarterly In-Person Training for Authorized Signatories	24
5.4.5 Drop-In Office Hours for Authorized Signatories	25
5.4.6 Require Authorized Signatories to Train Badge Holders	25
SECTION 6: STAKEHOLDER COMMUNICATION	27

6.1	Overview of Stakeholder Communication	27
6.2	Key Communication Considerations	28
6.3	Potential Communication Issues	28
6.4	Communication Processes, Practices, and Strategies to Consider	28
6.4.1	Publicly Available Information	28
6.4.2	Outreach Campaigns	30
6.4.3	Authorized Signatory Reference Guide	31
6.4.4	Authorized Signatory Responsibility Summary Sheet	32
SECTION 7: ENFORCEMENT		33
7.1	Overview of Enforcement	33
7.2	Key Enforcement Considerations	34
7.3	Potential Enforcement Issues	35
7.4.1	Diverse Penalties	36
7.4.2	Non-Monetary Penalties	37
7.4.3	Threshold for Company Penalties	38
7.4.4	Graduated Penalty Structure	39
7.4.5	Penalty Refund	40
7.4.6	Police Reports	40
7.4.7	Construction Contracts	41
7.4.8	Fixed Base Operators	41
7.4.9	Badge Return Moratorium	41
SECTION 8: BADGING OFFICE AND TRUSTED AGENTS		43
8.1	Overview of Badging Office and Trusted Agents	43
8.2	Key Badging Office and Trusted Agent Considerations	43
8.3	Potential Badging Office and Trusted Agent Issues	43
8.4	Badging Office and Trusted Agent Processes, Procedures, and Strategies to Consider	44
8.4.1	Expired Badges	44
8.4.2	Policies and Procedures	44
8.4.3	Situational Awareness	45
8.4.4	Internal Audit	46
8.4.5	Review Need for Secured Area Access	46
SECTION 9: AUDITING		48
9.1	Overview of Auditing	48
9.2	Key Auditing Considerations	49
9.3	Potential Auditing Issues	49
9.1	Auditing Processes, Procedures, and Strategies to Consider	49
9.1.1	Badge Control Through Auditing	49
9.1.2	Baseline Auditing	50

9.1.3	Problem Companies	51
9.1.4	Badge Accountability Through Auditing	51
SECTION 10: LOW UNACCOUNTABILITY TRENDS		52
SECTION 11: PHYSICAL ACCESS CONTROL SYSTEMS AND IDENTITY MANAGEMENT SYSTEMS		55
SECTION 12: RISK MITIGATION FRAMEWORK		56
SECTION 13: CONCLUSION		59
REFERENCES		60
APPENDIX A: POLICY ALTERNATIVE CHEAT SHEET		A-1
APPENDIX B: BADGE HOLDER BROCHURE		B-1
APPENDIX C: BADGE HOLDER FACT SHEET		C-1
APPENDIX D: ASAC ID MEDIA AUDIT RECOMMENDATIONS		D-1
APPENDIX E: RISK MITIGATION WORKSHEET		E-1
APPENDIX F: DHS INTEGRATED RISK MANAGEMENT		F-1

TABLES & FIGURES

Table 3-1. Factors that Affect ID Media Accountability and Control Policies and Procedures	7
Table 10-1. Airports with Unaccountability Below Two Percent	53
Table 10-2. Airports with Unaccountability Between Two and Three Percent	54
Figure 1-1. Airports Interviewed per Category	3
Figure 2-1. Considerations Resulting from the FAA Extension Safety and Security Act of 2016	5
Figure 4-1. Sample Airport Badge Holder Responsibility Sheet	12
Figure 4-2. One ID Media Considerations	13
Figure 6-1. Communication Tips	27
Figure 6-2. Public Information and Security Culture in Relation to Accountability	29

EXECUTIVE SUMMARY

Background

Airport-issued identification (ID) media accountability and control affects overall airport security. Improper management of ID media programs results in high percentages of badges that are unaccounted for, which causes a security vulnerability by weakening the access control systems (ACS) and amplifying the risk of insider threat. To mitigate these effects, airport operators must devise a robust and reliable approach to accountability and control that addresses complex regulatory requirements and overcomes diverse operational challenges.

Recognizing the challenges concerning ID media accountability and control, the National Safe Skies Alliance (Safe Skies) Program for Applied Research in Airport Security (PARAS) initiated a research project with the goal of assisting airports of all sizes to address, at a minimum, the following:

- Security controls during the issuance and renewal of ID media
- Methods for conducting ID media audits
- Procedures to mitigate lost, stolen, not returned, and unaccounted-for ID media
- Strategies to enhance ID media retrieval
- Trusted agent quality assurance/quality control processes

Goals and Objectives

Considering the objectives outlined by the Project Panel, the Project Team devised goals and objectives in key areas, as shown below:

ID Media Program	
Goal:	1.0 Identify how airports achieve successful ID media accountability programs through various processes, procedures, and strategies
Objectives:	1.1 Determine what internal and external factors affect accountability and control of ID media
	1.2 Match the appropriate processes, procedures, and strategies with the airport culture and mission
	1.3 Assess which processes, procedures, and strategies complement one another to achieve low unaccountability percentages
ID Media Issuance	
Goal:	2.0 Identify how airports can improve or implement procedures in the issuance process that enhance control of ID media
Objectives:	2.1 Determine whether certain processes, procedures, or strategies impact ID media accountability and control
	2.2 Assess whether the ID media issuance offers an opportunity to better communicate ID media responsibilities or to implement control strategies

Training

Goal:	3.0 Identify how to enhance training for badge holders and authorized signatories to improve ID media accountability
Objectives:	3.1 Determine whether a new badge holder or authorized signatory practice affects accountability
	3.2 Determine whether recurrent training for badge holders or authorized signatories can improve accountability
	3.3 Devise alternative training strategies for airports to use

Stakeholder Communication

Goal:	4.0 Identify whether communication practices affect accountability and control of ID media
Objectives:	4.1 Determine whether publicly available rules and regulations affect accountability
	4.2 Evaluate communication strategies that match the demands of airport communities

Enforcement

Goal:	5.0 Identify whether enforcement processes, procedures, or strategies affect accountability and control of ID media
Objectives:	5.1 Determine how monetary or non-monetary penalties affect accountability
	5.2 Determine whether the value of the penalty affects accountability
	5.3 Assess whether a combination of penalties can improve accountability

Badging Office and Trusted Agents

Goal:	6.0 Identify whether badging office and trusted agent policies, procedures, and practices affect ID media accountability and control
Objectives:	6.1 Determine whether written policies and procedures improve control
	6.2 Assess whether collection and penalization practices for expired ID media impact control

Auditing

Goal:	7.0 Identify whether auditing practices affect accountability and control
Objectives:	7.1 Determine whether auditing processes, practices, and strategies improve accountability and control

Project Approach

The Project Team interviewed 26 airports of various sizes to gather information concerning their ID media program accountability and control policies, and resulting unaccountability percentages. The interviews addressed the airports' unique processes, procedures, and strategies, with a focus on each airport's approach to controlling its badges.

The Project Team collected unaccountability information and comparable data to assess strengths and weaknesses across the airport. After reviewing the data collected, the Project Team outlined key findings related to ID media issuance, training, communication, enforcement, badging office and trusted agent

practices, and auditing. With these findings, the Project Team developed alternative options and assessed efficacy of each based on likelihood to achieve a policy goal and objective; efficiency in achieving the goal; administrative considerations; technology considerations; and acceptance and support among interested parties, including the airport community, airport leadership, and politicians.

Key Findings

Airport interviews revealed the following key findings affecting the success of airport-issued ID media accountability and control:

ID Media Program Balance

- Successful programs commonly had multiple key processes, procedures, and strategies in place that worked in coordination to consistently achieve low unaccountability.
- Successful programs had airport leadership support, and an understanding within the community that the airport prioritized the return of ID media.
- Airports with strong security cultures had strong control practices and often lower unaccountability percentages.

ID Media Issuance

- A badge holder responsibility sheet provides an opportunity to begin the training process with badge holders early, and can be used as support for later enforcement actions.
- Airports that set expiration dates for reasons other than an attempt to control unaccountability percentages had consistently low unaccountability percentages.

Training

- The research did not discern a difference in unaccountability percentages between airports that used computer-based and in-person training.
- Many trainees experience information overload during the training process.
- Alternative training strategies, such as peer-to-peer authorized signatory training, offer a way to successfully engage authorized signatories and badge holders.

Stakeholder Communications

- Despite regulatory training mandates, authorized signatories and badge holders consistently report a lack of understanding of their ID media responsibilities.
- Publication of rules and responsibilities can reduce the need for other efforts to educate authorized signatories and the badge holder community.
- Communications may come in many forms, but must have a clear objective, an understanding of the intended audience, and clear and concise language.

Enforcement

- High monetary penalties did not, on their own, guarantee consistently low unaccountability percentages for the airports interviewed.
- A mixture of monetary and non-monetary penalties can assist an airport in suppressing bad behavior and incentivizing good practices.
- Airports that hold companies liable for returning ID media have lower unaccountability rates.

Badging Office and Trusted Agents

- Airports that pursued ID media for a year or more after the expiration data had consistently low unaccountability percentages.
- Airports that prioritized security culture and security awareness in their airport community had written policies and procedures for the badging office, and consistently low unaccountability percentages.

Auditing

- Airport operators that manage their programs through their auditing practices achieve consistently low unaccountability percentages. These airports design audits to address a defined issue and act based on the audit findings.

Conclusion

Though multiple approaches can lead to lower ID media unaccountability, a successful approach involves matching the appropriate policy with the airport's mission and culture. Many airports implement one-off strategies without considering how such strategies will intersect with existing processes and procedures. This results in inconsistent approaches or short-lived trials that lack sufficient opportunity to take root. In contrast, airports with successful ID media accountability and control processes, practices, and strategies consistently demonstrated a balance of management interests, enforcement strategies, and communication strategies. For example, airports with a greater emphasis on security culture generally have strong badging office practices and infrequently use their enforcement actions.

Although all of the airports the Project Team identified as having a greater emphasis on security culture also had successful ID media control, this emphasis on security culture is not required to achieve low unaccountability. Other airports achieved strong accountability through other approaches. In summary, successful programs need not look alike or require the most resource-intensive policy options. Airports are advised to focus their efforts on the processes, procedures, and strategies aligned with their individual needs and goals.

PARAS ACRONYMS

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

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ACS	Access Control System
ASAC	Aviation Security Advisory Committee
ASP	Airport Security Program
ASP NA	Airport Security Program National Amendment
ASSIST	Airport Security Systems Integrated Support Testing
CBT	Computer Based Testing
CHRC	Criminal History Record Check
DHS IG	Department of Homeland Security Inspector General
ESRM	Enterprise Security Risk Management
FBO	Fixed Base Operator
GAO	Government Accountability Office
HR	Human Resources
ID	Identification
IDMS	Identity Management System
IRM	Integrated Risk Management
NASP	National Association of School Psychologists
PACS	Physical Access Control Systems
PARAS	Program for Applied Research in Airport Security
SeMS	Security Management Systems
SD	Security Directive

SECTION 1: INTRODUCTION

1.1 Overview

Airport operators of all sizes across the United States confront challenges in accounting for airport-issued ID media. These challenges date back to the late 1980s, with the introduction of regulatory measures to address access control policies and procedures. This guidebook discusses airport efforts to address the critical issue of ID media accountability and control. To aid readability, the terms ID media, badge, and credential will be used interchangeably throughout the document.

TSA oversees federal regulations that require airport operators to control access to secured areas of the airport, and establish an identification system that includes the issuance of ID media. This identification system must include measures to account for and control such media. Through subsequent regulatory measures, TSA imposes penalties and requirements for reissuance when a certain percentage is found to be unaccounted for during checks. Recently, the US Congress imposed enhanced reporting requirements and penalty provisions for airport operators and individuals who fail to properly account for ID media. The failure of airport operators to maintain accountability can result in TSA mandating additional operational requirements, fines, or penalties, which all have the potential to damage the airport's brand.

Airport operators' ability to maintain control of ID media is of interest to several external stakeholders, including TSA, the DHS Inspector General (DHS IG), Congress, and news outlets. For example, congressional interest in control of ID media remains high because of its perceived ability to prevent terrorist attacks. The 1989 Presidential Commission on Aviation Security and Terrorism's Bush Commission Report identified access media accountability as an effective measure to combat terror threats to airports and aircraft. As the FAA Extension Safety and Security Act of 2016 demonstrates, Congress continues to believe that unaccounted-for ID media presents a significant vulnerability to airport security. TSA also continues to consider regulatory changes for accountability and control.

1.2 Challenges Affecting ID Media Accountability and Control

Key government stakeholders' focus on this issue, combined with an ever-present potential for insider threats, means that airport operators must implement rigorous policies to minimize the number of unaccounted-for badges. Airport operators seek strategies to minimize unaccounted-for badges to avoid reissuance, newly mandated reporting requirements, and fines, in addition to the brand damage that follows. Irrespective of regulatory requirements, airport operators must remain vigilant and think creatively to control and account for ID media, and thereby maintain a robust security posture.

Challenges to controlling and accounting for ID media result from a dynamic set of factors, including:

- Regulatory complexities
- Diverse stakeholder populations
- Badge holders and authorized signatories neglecting their responsibilities
- Trusted agent errors or deviation from established procedures
- Failures of authorized signatory or trusted agent procedures
- Inaccurate audits
- Temporary employment
- High turnover of badge holders

Airports employ a variety of administrative procedures, training, penalties, auditing strategies, and communications campaigns to enhance control and reduce unaccountability. These measures lead to varying degrees of success. This guidebook assesses these measures and their value based on the unique operational demands of the airport environments in which they are deployed.

1.3 Research Approach

The Project Team began its research by identifying a set of questions that addressed the component parts of an ID media program, and the internal and external factors within an airport community that affect accountability and control. The questions include the following:

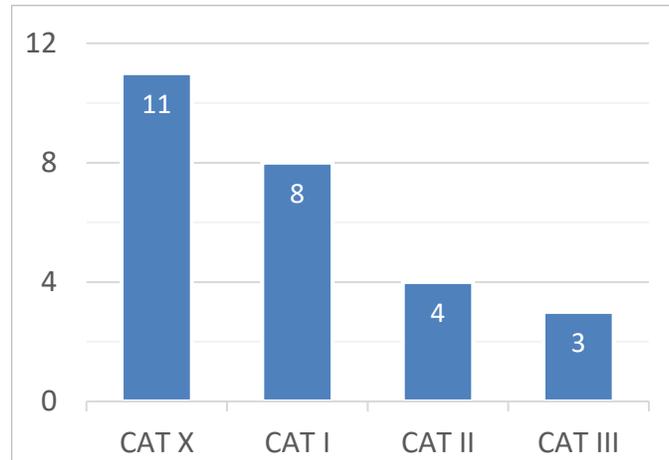
- Can the issuance process impact accountability or control?
- Does training affect accountability of ID media?
- Does public availability and accessibility of accountability policies and procedures affect accountability?
- Do monetary or non-monetary penalties, or a combination of both, affect accountability?
- Does imposing additional accountability measures on specified populations, based on propensity to return badges, affect accountability?
- Do express written rules for badge holders, authorized signatories, and trusted agents affect accountability?
- Do procedures of the badging staff or airport representatives responsible for accountability and control affect control?
- Does imposing requirements on the company or authorized signatory affect accountability?
- Do auditing practices affect accountability?

The Project Team then established the following criteria to evaluate the effectiveness of practices, processes, and procedures:

- Effectiveness – the likelihood of achieving policy goals and objectives
- Efficiency – achievement of program goals or benefits in relation to costs
- Equity – fairness or justice in distribution of policy costs, benefits, and risks across population subgroups
- Political – extent to which interested parties accept and support a policy proposal
- Social – extent to which the airport community will accept the policy proposal
- Administrative – likelihood the policy can be implemented
- Technical – availability and reliability of technology necessary to implement the policy

The Project Team then conducted a literature review to analyze key concepts relating to ID media programs, and began the airport interview process. The airport interviews proved valuable in exploring factors influencing accountability, and collecting data and program materials. The Project Team interviewed 26 airports during the project. Figure 1-1 outlines the number of airports interviewed in each category. The airport operators, whose information will remain confidential, answered questions regarding their programs, and provided data and documentation for the Project Team to analyze, providing further understanding of the policies that affect accountability and control. The interview topics covered during airport discussions included:

Figure 1-1. Airports Interviewed per Category



- Unaccountability rates
- Application processes
- Training
- Penalties and incentives
- ID media renewal
- Badging office and trusted agent practices
- Auditing
- ID media return
- Mitigation measures

1.4 Document Layout

Section 2 discusses the regulatory history of ID media requirements and how regulations and stakeholder interests have evolved. This information provides the context necessary to understand TSA's position, and assess the value of older policies and procedures.

Section 3 explores ID media accountability and control as part of a comprehensive policy. Successful programs employ complementary policy and mitigation measures with buy-in from airport leadership.

Sections 4–9 outline specific program areas. Some of these follow regulatory requirements, while others discuss non-regulatory practices that enhance control efforts. The sections include introductory discussions of each topic, and specific policy options an airport operator may consider implementing (see Appendix A, Policy Alternative Cheat Sheet).

Section 10 explores the trends identified in the strongest performing airports interviewed to outline how properly pairing measures achieves low and consistent unaccountability percentages.

Section 11 discusses how Physical Access Control Systems (PACS) and Identity Management Systems (IDMS) can impact accountability and control of ID media.

Section 12 looks at ID media control planning through the context of risk-based security, security management systems (SeMS), and risk mitigation. The research for this report has enabled the Project Team to develop a risk mitigation framework tailored to airport-issued ID media programs.

SECTION 2: REGULATORY HISTORY

Understanding the history of regulations concerning ID media accountability and control provides insights into probable focus areas for future regulatory activity. This understanding can assist airports in developing programs aligned with future federal regulations and the airport's individual identity. With over 30 years of federal regulatory activity regarding ID media, there is substantial information to guide airports looking to anticipate potential future requirements.

2.1 Automated Access Control, Human Factors, and ID Media Issuance

The origins of current regulations on ID media accountability trace back to Executive Order 12686, The Bush Commission Report. President George H.W. Bush commissioned the report in the wake of the bombing of Pan Am 103 in the skies over Lockerbie, Scotland on December 21, 1988. While much of the Bush Commission Report focuses on passenger and baggage screening issues, it also makes recommendations related to other security deficiencies. The Report notes the development of automated access control measures and the important security benefits those systems could provide. However, the report also emphasizes the importance of human factors and procedures for issuance and return of employee access badges for the operation of automated ACS.

In an effort to address shortcomings identified in the Bush Commission Report, Congress passed the Aviation Security Improvement Act of 1990. Among other provisions, the Act requires the implementation of measures that restrict unescorted access to secure areas to individuals who pass a fingerprint-based Criminal History Record Check (CHRC), and focuses on enhancing human performance in the aviation security system.

The resulting rulemaking led to a series of provisions on unescorted access, including Part 107.25 Airport Identification Media. This represents the first regulatory effort to address the human factors concerns articulated in the Bush Commission Report and the Aviation Security Act of 1990. This rule requires the airport to provide training for unescorted access credential holders, and to keep records of training provided to those granted unescorted access. The regulation does not specify any other recordkeeping or auditing requirements.

The findings of the Bush Commission Report, and the resulting legislation and rulemaking, identify two different but intersecting aviation security concepts: automated access control and the use of ID media. While these two matters are separate, they can and frequently do function together, for example, using a badge as an authenticating token for automated access control. However, the respective regulations of these two concepts remain separate.

2.2 Managing and Auditing Unescorted Access Identification System

Following the crash of Trans World Airlines Flight 800, President Clinton established a White House Commission on Aviation and Security. The Commission issued an initial report in September 1996 with 20 recommendations for improving aviation safety and security, and a final report in February 1997 that included 57 recommendations. Among its security recommendations, the Commission said that air carriers and airport authorities working with the FAA must secure controlled areas.

The White House Commission's recommendations led the FAA to propose an identification system to manage and audit airport-issued ID media that granted unescorted access to secured airport areas. This represented a significant shift to accountability from the education-based approach that was found in earlier regulatory measures. Instead of training, the proposed amendment focused on system audits and

operational compliance. Industry stakeholders argued against an annual audit requirement and pushed for a ten-percent unaccountability percentage threshold.

Of note, the Department of Transportation Inspector General published an audit report in December 2000, between the issuance of the proposed rule and final rule. The report assessed controls over airport ID media and identified the control of access to airports' secured areas as a topic of serious concern. The report found that the FAA did not take adequate steps to ensure that only trusted individuals could gain access to secured airport areas or that access was denied when it was no longer authorized. The report specified that airport operators "had not developed and implemented adequate procedures to account for airport ID and immediately deny access to secure airport areas when required." The report recommended that the FAA require airport operators and air carriers to audit the number of active ID media at least once per year. Additionally, the report suggested that the FAA issue standard audit procedures to ensure the effectiveness of the audits.

2.3 Better Accounting and TSA Oversight

In response to a February 2015 national news outlet report that missing airport badges could pose a security threat, the DHS IG assessed whether TSA adequately oversaw badge controls at airports to mitigate risk. The DHS IG concluded in report OIG-17-04 that airports do not always properly account for badges after issuance. Additionally, the DHS IG concluded that TSA relied on airport-reported information and inadequately inspected controls. The DHS IG determined that TSA could strengthen oversight by testing more controls and encouraging wider use of best practices by airports.

Congress addressed the issues identified by the DHS IG in the FAA Extension Safety and Security Act of 2016. The Act directs TSA to enhance oversight of airport access control and address ID media accountability as detailed in Figure 2-1. Congress directed TSA to consider increased fines, and additional audits and reporting requirements for airports. Some of these measures take effect when the accountability percentage rises to only three percent. This clearly demonstrates Congress's perceived risk of unaccountable badges.

Figure 2-1. Considerations Resulting from the FAA Extension Safety and Security Act of 2016

1. Increased fines for airports that report more than five percent of its unescorted access ID media for any SIDA missing
2. Best practices for Category X airports that report more than three percent of credentials for unescorted access to any SIDA missing
3. Additional audits and status checks for airport operators that report more than three percent of access media missing
4. Review and analysis of the prior five years of audits for airports that report more than three percent of access media missing
5. Increased fines and direct enforcement requirements for airport workers and their employers that fail to report within 24 hours an employment termination or a missing credential for unescorted access to any SIDA

TSA has used compliance efforts to alter how airports account for and control ID media, and address increasing concerns over insider threat. Additionally, in response to the FAA Reauthorization Safety and Security Act of 2016, TSA opted for two Airport Security Program National Amendments (ASP NA). These amendments enhanced authorized signatory training requirements and addressed auditing requirements. The auditing requirements will take effect in January 2020. Airport operators will need to

plan ASP changes that foster tailored processes, practices, and strategies that account for available resources and meet programmatic needs.

2.4 Planning for the Future

As airports look to improve their ID media programs, they should consider the implications of individual badge holder accountability requirements and the need for system-wide reviews of performance. Regulations have historically focused on training to improve individual badge holder accountability, and auditing practices to ensure the integrity of the system. Therefore, the interrelationship between badge accountability and ACS—particularly automated systems that utilize that badge—have been of significant regulatory interest to TSA. The development of technologies like biometrics that can enhance the identity verification of ACS may provide a future path forward to ensuring the integrity of access to secured areas without relying on individual accountability.

SECTION 3: ID MEDIA PROGRAM

Airports that successfully control ID media have adopted a myriad of processes, procedures, and strategies across their programs. This project’s research found that multiple alternative approaches can lead to effective control. The most successful programs match the appropriate processes, procedures, or strategies with the airport’s mission and culture in a balanced approach that maximizes accountability and control.

3.1 ID Media Program Balance

Similar to other business decisions, creators of airport ID media programs must consider their airport’s dynamic environment in developing a balanced strategy. Contingency management theory recognizes that no universally applicable method of organizational management or leadership exists. Organizational functions depend on a range of external and internal factors. To develop successful ID media programs, airports must understand how these factors impact airport control and stakeholder accountability. Table 3-1 identifies internal and external factors that will affect the success of accountability and control policy options.

Table 3-1. Factors that Affect ID Media Accountability and Control Policies and Procedures

Airport culture	How the airport community operates as a whole and interacts with the airport system
Security culture	A subset of airport culture; addresses the role security plays in the airport community’s daily operation
Airport mission, strategic plan, and leadership direction	Impacts the overarching policy strategy for the airport ID media program and the specific options it can deploy to mitigate accountability and control concerns
Political support	Political stakeholder support will affect the airport’s justification for policy options and the airport community’s response to enforcement or policy changes
Enforcement	Local and state regulations may enable or restrict enforcement policies, and impact the administrative burden to manage the program or change a policy
Policy flexibility	Airport policies differ in what can and cannot change without requiring entirely new policies and procedures
Other airport operational considerations	Regulatory requirements not related to badge accountability, and strategic plans and objectives that accountability policies will affect
Available resources	Funding constraints may impact an airport’s ability to implement resource-intensive mitigation measures
Tenant business practices	Tenants’ policies and priorities will impact how they manage their ID media
Airport contractual relationship with tenant	Airports may have contractual language in tenant agreements that enable certain controls of badge accountability
Local economy	Local economy will drive turnover of the badged population; some airports have long-tenured badge holders while others face significant turnover

3.2 Successful ID Media Program Commonalities

The airport interview process made it abundantly clear that ID media accountability and control processes, procedures, and strategies must complement one another to achieve low unaccountability percentages. For example, an audit that identifies companies with poor badge management practices will positively impact accountability only if appropriate corrective actions, such as enforcement or training, are taken to mitigate the issues identified. Similarly, if an airport reduces the amount of accountability training, other forms of community engagement and education should be employed.

With respect to corrective action, interviews reveal that many airports expect that higher penalties result in stronger accountability. However, the data collected shows that not all airports with high penalties achieve low unaccountability. Airports with low unaccountability and high monetary penalties had other policies in place—including other enforcement options—that supported their program. Similarly, airports with active enforcement of lower value penalties achieved consistently low unaccountability with training and outreach strategies.

Seven out of the 12 airports that reported active enforcement of higher penalties had consistently low unaccountability percentages. Three of the seven reported auditing strategies that met the regulatory baseline, but these airports did not use audit information to actively improve accountability. Instead, these airports had active communication strategies and strong security cultures; their badging offices had policies and procedures in place; and they all held companies and authorized signatories accountable through some form of non-monetary penalty. Additionally, these three airports reported that they set their renewal periods at one year because of FAA requirements, not accountability concerns.

In contrast, an airport with high penalty values but inconsistent and higher unaccountability reported poor communication strategies and security culture initiatives; self-driven on-the-job learning for badging office staff; a reliance on authorized signatories who were only provided support if requested; and an absence of engagement with the companies at higher levels. Furthermore, the airport has reduced sterile area badge renewal periods to prevent exceeding the reissuance threshold.

Two of the four airports that reported active enforcement of lower penalties had consistently low unaccountability. One of these airports had notably strong performance and reported no significant or unique efforts to achieve low unaccountability. This airport attributed their success to a strong internal security culture that the community takes pride in. The airport stresses security culture and security awareness at initial badge holder training, and it is consistently discussed within the community. The second airport with low monetary penalties requires companies with poor management practices to have reduced renewal periods until the company documents or otherwise demonstrates an improved management strategy.

Airports with varying monetary penalty amounts but consistent enforcement all reported that they had one or two other processes, practices, or strategies that assisted them in controlling accountability. These processes, practices, or strategies were connected in some way. For example, if an airport focused its efforts on authorized signatory engagement, they reported that their enforcement actions targeted the authorized signatory population.

Some airports reported trying a new process, procedure, or strategy without first considering the impact on measures already in place. This often led to either discontinuing the new practice before its impact could be measured and assessed, or implementing other measures that required additional resources to mitigate remaining issues. Many airports reported implementing some variation of a reduced renewal period to control rising unaccountability percentages, but did not have any other policies in place to address root causes, such as poor company or authorized signatory management practices.

When evaluating current initiatives or considering new ones, airport operators must take a holistic view. Consistent with contingency management theory, the airport must consider how internal and external factors will affect the proposed process, procedure, or strategy, and how it will complement other program measures. The airport can then tailor the process, procedure, or strategy to meet their specific needs.

SECTION 4: ID MEDIA ISSUANCE

The ID media issuance process offers opportunities for airports to improve their accountability and control. The TSA requires application forms to include specific content, that authorized signatories sign an acknowledgment of their responsibilities, and that the airport audits its processes and procedures.

4.1 Key ID Media Issuance Considerations

Creative airports take advantage of the following considerations during badge issuance. This helps airports begin the training process, establish relationships, and implement control strategies.

- The issuance process provides the airport with an opportunity to communicate with the applicant and sponsoring authorized signatory. The airport may provide either party with additional information regarding their responsibilities or security awareness.
- An airport can ensure the quality of data collected to assess and grant access privileges, and ensure data is input properly to maintain accurate records.
- An airport can impose controls on access privileges to impact accountability, such as setting an expiration date.
- Badge issuance has numerous required steps and processes. Airports must ensure that any additional steps or information do not infringe upon other goals and objectives. Overwhelming stakeholders with information may cause them to miss key points or make errors.

4.2 Potential ID Media Issuance Issues

- **Information overload.** Introducing too much information at once or requiring multiple signatures may convolute the application process and lead to data entry mistakes or stakeholders missing key lessons. New applicants receive an abundance of information from their employer and the airport as they begin their new job and apply for unescorted access authority. It is not practical to expect the applicant to retain actionable information at this time. As further discussed in Section 6, Stakeholder Communication, people typically retain two items at an actionable level from a communication. Therefore, airport operators must think about the amount of information they present to applicants, the methods by which they present it, and the results they want to achieve by communicating that information.
- **Expiration and renewal strategies.** Airport operators have used the badge expiration date to control accountability. Over the past few years, many airports have tested variations of this strategy to avoid unaccountability percentages that will trigger reporting or reissuance requirements. While this report draws some preliminary conclusions about renewal strategies, the airport community may benefit further from a more in-depth look at the value of these strategies.

4.3 ID Media Issues Processes, Procedures, and Strategies to Consider

The following process, procedure, and strategy options offer ways for an airport to use badge issuance to enhance controls and initiate badge holder training.

4.3.1 Standard ID Media Application

Include only basic authorized signatory and badge holder responsibility language in the ID media application.

Airport operators can choose to provide basic responsibility language in the ID media application. Most often, this includes language that the badge is property of the airport authority, that the badge holder must immediately report if it is lost or stolen, and that it must be returned to the airport authority when unescorted access to the applicable secured area is no longer needed. The authorized signatory must attest that the applicant has a need for access and is aware of their security responsibilities as defined in 49 CFR § 1540.105. The airport may supplement this requirement by having the badge holder sign the document and acknowledge their ID media responsibilities.

Advantages:

- **Simplified application process.** Airport operators may consider this policy option to simplify the ID media application. Some airports have lengthy applications that require various acknowledgments of rights and responsibilities. Additionally, the airport, applicant, and authorized signatory all have other priorities during the ID media issuance process. This option delays an airport's effort to highlight authorized signatory and badge holder responsibilities and focuses on ensuring accurate data is collected in the application. The applicant and authorized signatory can devote more attention to the application content and the accuracy of the data they provide. Similarly, the airport's badging office will benefit from a streamlined process.

If adopting this policy option, an airport should consider other strategies to ensure new badge holders and their respective authorized signatories receive necessary accountability information. Airports may therefore consider communicating responsibilities through a combination of training, airport engagement, and authorized signatory or company outreach strategies.

Alternatives:

- **Detailed application.** Airport operators can include more specific accountability instructions and penalty information in the application. These airports can point to the information provided in the application packet to support enforcement activities. However, choosing this option will add information to the application and increase the possibility that the applicant or authorized signatory may ignore or forget important content. Similarly, the applicant or authorized signatory may make data entry errors due to application length.

Airports that adopt this strategy may choose to implement less robust training or outreach campaigns, but must ensure other management or enforcement activities support the strategy.

4.3.2 ID Media Applicant Responsibility Sheet

Require the applicant to sign an responsibility sheet before issuing the badge.

An airport operator may provide the applicant with a responsibility sheet, separate and apart from the application, that focuses on badge holder accountability responsibilities. The sheet should succinctly cover badge holder responsibilities and penalties for noncompliance. Information provided should tell a badge holder what to do if they lose their badge, if it is stolen, or if they no longer need access to the secured area. Additionally, the sheet can include other ID media-related security responsibilities, as long as the responsibilities sheet remains short and succinct (not to exceed one page). The sheet should resonate with the badge holder and trigger action where appropriate. Figure 4-1 provides an example of such a sheet.

In addition to informing applicants of their responsibilities, the sheet can assist the airport operator with enforcement actions. Airport operators report that badge holders frequently claim they were unaware of their responsibility to report lost or stolen badges. Importantly, airport operators must follow through with enforcement to ensure the sheet remains relevant.

The airport operator may require badge holders to retain this sheet and return it when they renew their badge.

Advantages:

- **Emphasized responsibilities.** Providing the sheet separate from the application draws attention to it and offers an additional opportunity to highlight the importance of safeguarding and returning the badge. As discussed earlier, the applicant receives an abundance of information as they start a new job and learn the operating rules and procedures at the airport. Separating the information and providing it at a different time increases the likelihood of retention.
- **Supplemental information.** The responsibility sheet can supplement an application that covers basic information. The second document can include additional context to assist the badge holder in comprehending and later applying the lesson. This approach may help the applicant pay closer attention to the details of each document. An airport can distribute and require signature of the responsibility sheet at a different point in the process when the applicant may not have as many documents to sign and submit. For example, the airport can require the applicant to return the sheet with the application package, or sign the sheet at a separate time, potentially while retrieving the badge after approval.
- **Amendable.** Altering a supplemental responsibility sheet will not require the same time-consuming approvals as changing the application. Therefore, the airport will have the ability to adjust the responsibility sheet as they deem necessary to reflect change recommendations, a shift in focus, and other necessary modifications.

Figure 4-1. Sample Airport Badge Holder Responsibility Sheet

Airport Badge Holder Responsibilities	
The ID media is property of the airport.	
Do not allow anyone else to use your ID media.	
Notify your authorized signatory or the airport immediately when your ID media is lost or stolen.	
Search for your lost ID media.	
File a police report for stolen ID media.	
Return the ID media to your authorized signatory or the airport badging office immediately when access is no longer needed.	
A violation of these responsibilities will result in a fine of \$250.00	
The airport will not issue a new ID media to an individual until the old ID media is returned or properly documented as lost or stolen.	
_____	_____
Badge Holder	Date

- **Notice.** The responsibility sheet can support enforcement action. Badge holders often claim ignorance of their responsibilities. The airport can use the issuance of the sheet as notice to the badge holder of their responsibility.
- **Security awareness.** The responsibility sheet may assist the airport in enhancing security awareness and security culture at the airport. Providing the sheet to the badge holder lets them know that the airport takes security seriously.

Alternatives:

- **Training and outreach.** Airport operators can provide additional information in the ID media training or through other outreach strategies. Recognizing the need to provide additional information, an airport can conduct its outreach at a different time than badge issuance.
- **Authorized signatories.** Airport operators may rely on the authorized signatory to provide responsibility information to new badge holders. This strategy relieves the airport of the administrative burden to create and distribute the sheets, does not add a new component to the ID media issuance process, and puts liability on the authorized signatory. An airport choosing this option must have a strong core of authorized signatories who display strong management practices. The airport may have to support the authorized signatories in this effort.

4.3.3 One ID Media

Issue only one badge to individuals who work for multiple employers.

Airports may choose to issue only one badge to individuals who work for multiple employers. Airports use this strategy to reduce exposure and enhance security. With only one badge, these individuals will not be able to access secured areas if they lose it, whereas a person with multiple badges may lose one and use another to access the secured area. Similarly, if a badge is unaccounted for, multiple sponsoring companies have an interest in its return, as all companies are responsible for their employees. This policy enhances security and eases the airport's administrative burden if the badge holder commits a security violation, because the airport only needs to deactivate one badge.

Airports can simplify management of this strategy by making all companies liable for security violations and ID media accountability. Therefore, multiple companies have an interest in taking the necessary measures to account for and recover the missing badge. Other considerations are outlined in Figure 4-2.

Airports that use this practice report that it simplifies the ID media management process. In the opinion of these airports, the badge holder has the burden to responsibly manage their badge and get the proper signatures from authorized signatories. Additionally, some IDMS companies have recommended that airports implement this strategy to simplify their management process. Having only one badge issued per individual makes it easier for some IDMS to manage ID media.

Figure 4-2. One ID Media Considerations

- Highest level of access controls
- All companies liable for accountability and security violations
- Shortest renewal period controls
- If add or drop a company, all companies must sign application for new badge

In considering whether to adopt the measure, some airports expressed concern with the different access levels that the badge holder's jobs may require. For example, a person working one job with access to the Security Identification Display Area (SIDA) and another job with access limited to the sterile area

may abuse the SIDA access privilege while working for the company sponsoring the lesser level of access. This is a reasonable concern, as it can be difficult to know whether a person is in the correct area to perform their work function. To help counter the potential for abuse, airports that have implemented this process issue violations to personnel found to be misusing access privileges, and all companies sponsoring those personnel.

If the badge holder needs to add or remove an employer, they will have to reapply for a new badge and have all authorized signatories sign the documentation. In this respect, the badge holder has greater responsibility for the management of their access authorization because they must ensure that all companies they work for complete necessary administrative processing. As a result, the airport's administrative burden will potentially be reduced. Airports will only have to turn off access for one badge to reflect status changes rather than processing multiple applications or renewals.

The renewal period for the badge can default to the shortest renewal period within the string of authorizations. For example, if authorization has a renewal period of two years and another has a renewal period of six months, the badge will expire in six months for both levels of access, and both companies will have to sign a renewal request.

Advantages:

- **Risk exposure.** Issuing one badge to individuals who work for multiple companies reduces airports' exposure to risk. If a security violation occurs, the airport only needs to revoke access for one credential. This strategy removes the potential for the credential holder or another individual to use additional badges to access secured areas.
- **Unaccountability exposure.** Issuing one badge to individuals who work for multiple companies reduces an airport's exposure to greater unaccountability. If the badge becomes unaccountable for any reason, only one is unaccountable, and several companies will be responsible for its return.
- **Administrative efficiency.** One badge can increase administrative efficiency for the badging office. Only one application needs to be processed and managed by the airport. Airports that have successfully adopted this strategy have found that badge holders take more responsibility for their credential as they must ensure that all authorized signatories complete necessary processes and procedures to keep their access up to date.

Alternative:

- **Multiple ID media.** Airports can issue multiple badges to individuals who work for more than one company. Airports may choose this option if a small percentage of the badged population works for multiple tenants. This approach may also work better for the airport's management processes or IDMS.

4.3.4 ID Media Expiration Periods

Set renewal periods based on operational concerns other than accountability.

Airport operators may set their renewal periods based on operational concerns other than accountability. An airport operator may consider local rules and regulations, FAA requirements (e.g., the yearly training requirement to operate a motor vehicle in an aircraft movement area), or administrative concerns that do not relate to accountability when determining the best renewal period. For example, the airport operator

may have a limited capacity to process renewals or provide recurrent training, and therefore may choose a two-year renewal period to disperse demand. Alternatively, the airport may find it easier to process FAA driving requirements or to manage recurrent training programs with one-year renewal periods.

Out of the 26 airports interviewed, 13 airports reported renewal periods of one or two years. Most often, these airport operators set renewal periods for reasons other than accountability, such as costs, training, or other operational needs. Ten of these airports reported low unaccountability percentages, and nine reported that percentage is consistent year after year and within the year. Airports that choose this approach use other policy options to control ID media.

Advantage:

- **Operational decision-making.** Airports can match their ID media expiration period with administrative or other operational needs. Controlling accountability with other processes, procedures, and strategies will enable the airport to set expiration periods that match their resource availability and operational needs.

Alternative:

- **Reduced or graduated expiration periods.** Implement a reduced expiration period or graduated renewal period. These strategies seek to control accountability through the expiration process.

Reduce ID media renewal periods to less than a year.

Airport operators can reduce renewal periods to less than a year to assist with controlling accountability. Airports may choose to apply the renewal period across the board, for specific access areas, or for specific companies based on issues like turnover or as a penalty for past high unaccountability rates. Shortened periods were also used for initial issuance of badges. Where an individual is a first-time applicant for unescorted access, the renewal period on the initial issue was shorter than the period for subsequent renewals.

An airport implementing this strategy will need support from airport leadership because the tenant community may resist due to the increased processing costs they will incur.

This option may also increase an airport's administrative burden to process renewals and issuance costs. However, some airports reported that they did not see any additional costs or demand on their badging office after reducing renewal periods for an entire access area, badged population, or for companies with poor performance. These airports reported that these populations or companies have high turnover, which requires processing by the airport on a regular basis regardless of the shortened renewal period.

Advantages:

- **Mitigate rising unaccountability.** This policy option can provide relief from the risk of reissuance, but does not necessarily enhance accountability or control. Many airport operators with shortened renewal periods reported that their unaccountability percentage is expected to change in the near term, or had recently changed because of the shortened expiration period. These unaccountability percentages therefore vary significantly based on the length of the renewal cycle. This process only removes badges from the unaccountable list because they expire. Airports employing this approach may consider other accountability and control

strategies to manage the process, and avoid risk associated with the ebb and flow of the renewal cycle.

- **Enforcement tool.** Airports can use this strategy as a non-monetary enforcement tool. An airport can subject companies with poor accountability management practices to shortened renewal periods. The company can receive relief from this penalty by either improving accountability over time or submitting a management plan to the airport. The airport can make the enforcement decision based on data collected from an audit or other observations, such as repeated return of badges in bulk, showing poor management practices, and an indifference to the airport's return requirements.

Alternatives:

- **Operational based decision making.** Implement an expiration period based on other operational needs. Airports may choose this process when they have other measures in place that control accountability.
- **Graduated ID media renewal period.** Implement a graduated renewal period. Airport operators may consider this measure if their longer tenured badge holders demonstrate stronger accountability practices.

Implement a graduated renewal period.

Graduated renewal periods operate similarly to graduated penalties. The badge holder receives an extended renewal period each time they return a badge. Airport operators can implement this policy option for all access media, specific access areas, specific classes of badge holder, or to penalize a company with accountability issues. Some airports shorten the renewal period for an individual if they lose their badge. The badge holder then can earn back their extended renewal period by successfully renewing the new badge without losing it again.

An airport must consider whether they can manage the increased burden of a graduated renewal process.

One airport interviewed conducted a risk analysis before implementing shortened initial renewal periods for new sterile area badge holders. The policy they were considering required new applicants to receive an initial six-month badge, and would then graduate to the airport's standard two-year renewal period after the initial renewal. The study demonstrated that 50 percent of the sterile area concessionaire employees turned over within the first six months of employment, and 75 percent turned over within the first year. The airport shared this risk analysis with sponsoring companies before issuing a new policy to illustrate that the policy change would not adversely affect those companies financially.

Of the 26 airports interviewed, 12 reported a graduated renewal period. Of those airports, seven reported their unaccountability rate varies year after year and within the year. Three of the airports with graduated renewal periods reported low unaccountability percentages at the time of the interview. These three airports reported their unaccountability percentage as consistent year after year and within the year.

Airport leadership support is important to ensure the tenant community accepts this strategy option.

Advantage:

- **Mitigate high turnover.** This strategy assists airports that experience high turnover of new badge holders, but requires additional accountability and control strategies for tenured badge holders. A short-term benefit will be having unaccountable expired badges drop from TSA's radar. The strategy will also reduce the airport's processing burdens and costs for tenured employees.

Alternatives:

- **Operational based decision-making.** Implement an expiration period based on other operational needs. Airports may choose this process when they have other measures in place that control accountability.
- **Reduced ID media expiration period.** An airport will benefit from a reduced expiration period where tenants have poor management practices and the airport has high turnover. Similarly, the airport may benefit from the simpler administrative process of a consistent expiration date rather than managing a graduated process.

Require ID media for seasonal employees and temporary contractors to expire on their last day of work.

An airport operator may issue a badge for seasonal employees or temporary contractors with an expiration date set for their last day of work. Seasonal workers often know when their work period will end. Similarly, a contractor will often have a specific date at which point they must have their work completed. Airports have found that setting the expiration date to the last day of work or providing a one-month grace period helps them manage these populations.

Some airport operators report that it is easier to renew a badge for a shortened amount of time than it is to find unreturned media. Other airports have chosen to issue normal renewal periods to these populations. In these cases, the administrative load of renewing for extensions was found to be burdensome. In some cases, these airports hold badges for seasonal employees who they know will return the following year, to avoid the difficulty of reissuing.

Some airports store badges for seasonal workers in lockboxes until the person returns. In most instances reported during the airport interviews, the seasonal workers were employees of the airport authority. However, some airports reported that they would collect and store contractor or tenant badges until the person returns to the airport for work again.

Advantage:

- **Leverage expiration date.** Setting seasonal and temporary contractor badges to expire at the end of the contract will reduce an airport's burdens with respect to recovery and TSA's unaccountable list. Seasonal and temporary contractor badges can represent a significant number of media issued, depending on the location of the airport and ongoing projects.

Alternative:

- **Standard expiration periods.** Set a standard expiration period and penalize the tenant or contractor for non-return. This strategy relieves the airport of the administrative burden connected to renewing or reissuing badges to seasonal employees or contractors who require access for longer than initially requested. Similarly, some seasonal workers may return within a standard expiration period and would not require renewal or issuance. Penalties can compel return of these badges. See Section 7 for additional enforcement discussions.

SECTION 5: TRAINING

5.1 Overview of Training

ID media programs require training of the authorized signatories and badge holders to achieve accountability success. An analysis of, and adjustments to, an airport's training policies can offer benefits to accountability. An effective training strategy balances the burden of training with the need to keep information fresh in the minds of key audiences.

Training can take many forms, and training regimens can vary widely. They can target a specific audience, such as badge holders, authorized signatories, companies, or trusted agents, as well as apply across the board. They can also vary in content coverage for different audiences or for type of training, such as initial, recurrent, or supplemental training.

TSA requires airports to train individuals before granting unescorted access to secured areas or SIDA. Many airports also offer training for badge holders with access to the AOA and sterile areas. Some airports have chosen to provide additional recurrent training to badge holders on a biannual, annual, or more frequent basis. TSA also requires that airports train authorized signatories on an annual basis. Airports frequently supplement these trainings with personal meetings and by distributing written information.

Airports accomplish initial and recurrent training in many ways, including in-person training, computer-based training, and a combination thereof. Airports may use pre-packaged training content, tailor pre-packaged training content, or create their own training content. The training can be generalized or targeted. For example, some airports provide generalized training for all badge holders and additional targeted training for authorized signatories.

In addition to more traditional training efforts, some airports offer or require supplemental training efforts that provide significant value in educating various populations within the airport community. As discussed in this section and throughout the policy options included in this guidebook, supplemental training could include spot training for different groups of badge holders, refresher training offered in person or online, company training, or other communication efforts that discuss accountability. Airport operators should consider the timing of these training efforts in relationship to that of their traditional and supplemental training efforts.

Training research offers helpful insights into what an airport operator should consider when thinking about changes to their training program. Studies have found that one-size-fits-all, fixed-date approaches to training are inadequate across an array of domains and contexts. Rather, optimal training is tailored for the objective and its audience. In an airport, the authorized signatory community may benefit from training that covers different requirements, whereas a badge holder may benefit from training that focuses on specific responsibilities targeted to their daily experiences. Communication strategies discussed in Section 6 also elaborate on this concept.

Many studies document that skills deteriorate as early as two months after training. Therefore, a one-and-done training approach is not effective because it ignores the well-documented realities of human cognition and performance. The temporal distribution of practices affects understanding and retention of knowledge. The way a person studies and learns information shapes how well that individual will remember the information in the future. Timing training sessions appropriately could save the airport resources by reducing the amount of unnecessary training, and streamlining the information to make it more efficient. Employees will better recall their training and apply it to their daily job functions. Of

course, an airport must consider the cost of such training. This includes not only the cost of offering the training but also the cost for companies sending their employees to receive the training. Accordingly, an airport should consider mechanisms like online training and programmed learning if pursuing a recurrent training regimen.

New badge holders and new authorized signatories receive an abundance of information from their employer and from the airport when they start a new job and apply for an access badge. Providing focused training on badge accountability a few weeks or months after the employee or authorized signatory begins work may help them retain and apply the information. An airport can offer additional training to supplement existing new badge holder training, or require authorized signatories to provide additional training to their badge holders.

Research has found that learning is more stable when training is spaced further apart in time. Learners are also better able to recall information and concepts if they are presented in multiple, spread-out sessions. This is known as the spacing effect, and it applies across all age-groups and a wide variety of skills. Several theories support the spacing effect. For example, deficient processing theories explain that people dedicate less attention to subsequent trainings if they occur too close in time. Therefore, inserting space between lessons helps ensure that people attend to and process the information discussed in the training. Numerous other theories discussed throughout this section support the spacing effect. They all emphasize that conducting smaller training sessions over time achieves higher rates of retention than one large training session.

However, as per contingency management theory, the effectiveness of training depends on a variety of factors. An airport must consider its community, resources, and vulnerabilities in prioritizing training. Airports will not all benefit from the same training media.

Consistency in training can also help reinforce the importance of security and accountability to employees. Covering information repeatedly reminds employees of its significance. Furthermore, regular training sessions present an opportunity to notify badge holders of policy changes.

5.2 Key Training Considerations

- Initial badge holder training includes numerous topics mandated by regulation and may not present the best opportunity to ensure badge holders know and remember their accountability responsibilities.
- Recurrent training for badge holders and authorized signatories helps to strengthen the airport security culture.
- An airport must consider how additional training for badge holders or authorized signatories will impact the overarching airport policies and airport leadership positions.
- The tenant community and business practices will impact the need for more or less training.
- Additional training initiatives may foster positive change in the airport security culture.

5.3 Potential Training Issues

- **Information Overload.** Introducing too much information at once during training may convolute the message and lead to employees missing key lessons. Initial badge holder training includes numerous topics mandated by regulation. A trainee may not effectively retain supplemental badge accountability information. Therefore, airports must think about how much information they want to present to badge holders in training, how and when it is presented, and what result they want to achieve by communicating that information.
- **Resource Constraints.** Offering recurring training may help prevent issues related to information overload. However, recurring training can strain airport resources. Airports may have limited space, technology, or staff hours available for training. Airports in this category must consider alternative ways to educate badge holders, such as through outreach campaigns.
- **Disengaged Authorized Signatories.** Supplemental trainings may assist an airport with poor authorized signatory practices. To improve results, the authorized signatories must engage and modify behavior based on the training.

5.4 Training Processes, Procedures, and Strategies to Consider

The following process, procedure, and strategy options offer ways for an airport to use badge holder training to enhance controls and badge holder accountability.

5.4.1 New Badge Holder Training

Cover only basic badge holder responsibilities in new badge holder training.

An airport operator may consider covering the core concepts of ID media responsibilities at a high-level in the required new badge holder training. The training should make the badge holder aware of their responsibilities, including that the badge is property of the airport; the airport must receive notification immediately when the badge holder no longer requires access; the badge holder is responsible for returning it to the badging office within a specified period of time; and the badge holder is responsible for notifying the badging office immediately if it is lost or stolen.

New badge holder training covers information required by regulation, and an airport may elect to add local information. New badge holders may become overwhelmed by the information. Research has found that memory retrieval strength is affected not just by time but also by interference with other information. As discussed in Section 6, a badge holder may not absorb all the information at a level that allows them to recall and apply the information as needed.

Airport operators may provide initial training either in person or as computer-based training (CBT). The airport interview findings did not show an appreciable difference between CBT or in-person training outcomes.

In-person training offers an opportunity to focus on security awareness and culture to a greater degree. CBT offers an efficient way to train, test, and manage training. In addition, training videos and CBT allow employees to learn at their own pace. Some airport operators implement pre-packaged training content, while others edit that content to add airport-specific information. Airports reported that their CBT modules translate easily to recurrent training.

Some airports prefer in-person training to educate new badge holders. In-person training allows the trainee to focus on specific topics based on the response of the training group. Most often, airports with in-person training reported using content specific to their internal rules and regulations, with a focus on security culture. But, the content of each class may vary slightly based on the trainer's focus. This strategy also requires the airport to have staff hours available to provide the training.

Airports choosing to provide basic information should consider supplementing the initial training with other training opportunities or communications activities that discuss accountability, badge holder responsibilities, and the role of the authorized signatory. The additional communication presents the opportunity to reinforce accountability topics and provide greater detail as necessary.

Advantage:

- **Introduce information.** New badge holders have to intake a lot of new information and lack context related to the lesson. Covering basic ID media responsibilities during training simply notifies the individuals that the issue is important and sets groundwork for additional training and communications.

Alternative:

- **Thorough coverage.** Airport operators may opt to provide thorough information during initial training to ensure the badge holder receives all necessary information. This may be an attractive option for airport operators that have resource constraints that limit their ability to provide additional training. Similarly, an airport will benefit from this option if they choose not to provide additional training because of strategic policy decisions.

5.4.2 Recurrent Training

Require recurrent training for all badge holders that includes reinforcement of ID media accountability responsibilities, penalties, and security awareness.

To enhance accountability, an airport operator may consider recurrent training for all badge holders that includes accountability and security awareness topics. The training should overview responsibilities, penalties for noncompliance, and why accountability matters. This policy option necessitates additional resources for the airport to provide training, including space, equipment, and time for badge holders. Additionally, this policy option will add an administrative burden to manage the recurrent training and recording keeping.

Recurrent training is especially important for retaining information that does not typically arise during day-to-day activities. A badge holder's recollection of policies and procedures will degrade if not frequently applied or reinforced. For example, a badge holder may have retained proper control of their badge between their initial training and renewal, but they may have forgotten the proper procedure for a lost badge because the issue has not occurred. Refreshing their understanding of the policies and procedures will ensure they know their responsibilities and may increase their vigilance to protect their badge.

Capitalizing on the spacing effect by ensuring information is repeated over time will reinforce initial training. During later training sessions, the individual will also have context from time on the job to support retention and understanding. This makes forgetting responsibilities less likely while increasing the likelihood of performing responsibilities when necessary.

With recurrent training, airports must also consider the frequency at which they want to offer the training. Research suggests that increasing the time between training opportunities is beneficial to a point, after which it begins to impair final retention. Alternatively, people will dedicate less attention or effort to encode a presentation if it is too close to the previous one. Therefore, inserting space between repetitions ensures that people can adequately attend to and process each one. Increasing the space between repetitions also reduces the burden on the new badge holders and the managers administering the training. In addition, as the space between trainings increases, the redundancy of contextual elements decreases. This enhances retention as per the encoding variability theories described in the previous subsection. Having more varied contextual information associated with the new information provides more routes in the brain through which that information can be accessed. Finally, the retrieval of past presentations of an item strengthens the original memory trace. The more difficult the retrieval, the more beneficial it is to memory retention. However, trainings should not be spaced so far apart that trainees cannot retrieve past presentations. Therefore, increasing the time between trainings is only beneficial to the point that these trainings can be recalled, beyond which their effectiveness is diminished.

Understanding the errors that the badged population make in regard to accountability and security awareness will assist the airport in assessing the appropriate frequency of recurrent training. The type, timing, and frequency of the errors will assist the airport in learning how the community is retaining and applying responsibility and security awareness information. The airport can then determine whether to require recurrent training on a more or less frequent basis for badge holders.

The airport will have to consider what content they would like to present in the recurrent training. They may choose to include the same content as initial training, additional topics, a shortened version of the initial training, or an adaptive training program that adjusts based on trainee responses. Airports should consider the frequency of recurrent accountability training in relation to other content, and the retention of information by the trainees. The airport can then adjust other strategies accordingly.

Recurrent training may strain resources. Airports may have limited space, technology, or staff hours to offer recurrent training for all badge holders. Some airports have spread out recurrent training requirements to ease this burden. For example, an airport that has shortened renewal periods requires recurrent training every two years rather than at every renewal.

Airports using recurrent training should consider tailoring the training to support their security culture strategies.

Advantage:

- **Increased retention.** Individuals better retain information when it is learned in multiple sessions. Recurrent training refreshes a person's awareness of their responsibilities and covers topics that may not have been confronted in the course of their employment.

Alternative:

- **Non-recurrent training.** Airport operators can choose to not provide recurrent training for all badge holders. This option will succeed if the authorized signatory provides adequate oversight of or training to their badge holders, if the airport has a strong security culture, or if the airport conducts outreach campaigns to educate badge holders.

5.4.3 Peer-to-Peer Authorized Signatory Training

Facilitate voluntary peer-to-peer authorized signatory training and strategy meetings biannually.

Voluntary peer-to-peer authorized signatory training presents an opportunity for authorized signatories to share best practices among themselves. This strategy may help airports with high authorized signatory turnover or with companies that routinely fail to manage their badged populations. The authorized signatory community will benefit by creating an open dialogue, and potentially creating an avenue to share best practices and brainstorm.

Of note, differences in tenant business practices may affect the value of the training. If the management practices of the tenants vary significantly, the discussions may not result in fruitful policy changes for the trainee. It may take some effort on the airport's part to get a disengaged authorized signatory community to participate. The authorized signatories have other responsibilities and may not prioritize badge accountability. However, a few successes may eventually lead to a larger, more impactful initiative.

Advantage:

- **Enhance security culture.** The discussion among peers will build a sense of ownership and responsibility among the community, and ideally engage those who have neglected their responsibilities.

Alternatives:

- **Annual authorized signatory training.** Airport operators can use the annual authorized signatory training to discuss best practices, management approaches, and any common challenges they see in the authorized signatory community.
- **Quarterly in-person training.** The airport can host biannual or quarterly meetings for authorized signatories to discuss best practices, management approaches, and any common challenges they see in the authorized signatory community.
- **Drop-in office hours for authorized signatories.** Office hours can provide authorized signatories an opportunity to visit the badging office to request assistance or advice from the airport if needed.

5.4.4 Quarterly In-Person Training for Authorized Signatories

Offer quarterly in-person training for authorized signatories.

Offering quarterly in-person authorized signatory training may assist airports in promoting greater vigilance among the authorized signatory community. The training exercise can supplement the yearly required training, and provide an opportunity to reinforce concepts, introduce new strategies, and potentially enhance the security culture.

Advantages:

- **Reinforces the importance of ID media responsibilities.** An airport with a disengaged authorized signatory community may require this additional training to remind them of the need for vigilance and improved practices.

- **Enhance security culture.** Requiring authorized signatories to take extra training will enhance the security culture.

Alternatives:

- **Rely on annual authorized signatory training.** Airports must provide training for authorized signatories on a yearly basis.
- **Raise pertinent issues at stakeholder meetings.** Airports can use stakeholder meetings to raise issues.

5.4.5 Drop-In Office Hours for Authorized Signatories

Offer drop-in office hours for authorized signatories to meet with the airport trusted agents to discuss badge accountability management practices.

An airport badging office may consider offering open office hours for authorized signatories to ask questions and receive management advice. This strategy can supplement efforts to engage authorized signatories and assist those with poor management practices. The office hours can occur once a quarter, once a month, or once a week, depending on the airport's resource availability and demand from the authorized signatory community

Advantages:

- **Preempt larger issues.** This strategy gives authorized signatories or companies a chance to come forward to the airport with concerns before a larger issue develops.
- **Enhanced security culture.** Drop-in office hours may help enhance the security culture.

Alternatives:

- **Rely on annual authorized signatory training.** Airports must provide training for authorized signatories on a yearly basis.
- **Raise pertinent issues at stakeholder meetings.** Airports can use stakeholder meetings to raise issues.

5.4.6 Require Authorized Signatories to Train Badge Holders

Require authorized signatories to discuss badge responsibilities with their badge holders monthly or quarterly.

An airport operator may require their authorized signatory to discuss badge holder responsibilities with their badged population monthly or quarterly. This does not require an extensive training session, but merely a discussion between the authorized signatory and their badge holders. For example, the authorized signatory may discuss the topic during a shift staff meeting or on an individual basis. The airport may consider providing content for the authorized signatory to cover. This type of training will supplement initial and recurrent training efforts.

By reviewing the information with new badge holders at separate times, the badge holders will have more opportunity to associate contextual elements with the information. This supports the encoding

variability theories as the storage of more varied contextual information provides more routes through which the target stimuli can be accessed later.

Advantage:

- **Minimal administrative burden.** This strategy does not require a massive time commitment on behalf of the airport operator or the authorized signatory, but the supplemental training can still help with memory retention.

Alternatives:

- **Provide recurrent training to badge holders.** Recurrent training provides the airport with the opportunity to re-engage the badge holders.
- **Publish ID media rules and responsibilities.** Providing rules and responsibility information publicly can assist badge holders in addressing issues on an as-needed basis.

SECTION 6: STAKEHOLDER COMMUNICATION

6.1 Overview of Stakeholder Communication

Communication underlies the success of airport ID media control. Of the airports interviewed, those with effective communication strategies in place had consistently low unaccountability percentages. Along with specific policy options discussed below, the overarching concepts discussed in this section apply to all aspects of badge accountability discussed in this report.

Airports should tell the community specifically what they want them to do and let them know the consequences of their actions from both a risk and penalty perspective. Instrumentality theory, further discussed in Section 7 (Enforcement), argues that people need to know specifically what they need to do, believe they can meet the goal, and understand that compliance is worthwhile. Therefore, an airport should create a communication strategy to control accountability that discusses the how and the why.

Figure 6-1. Communication Tips

NASP Effective (and Easy) Communications: Tips for School Psychologists

- Identify audience
- Tailor to audience
- Use clear and concise language
- Set an objective
- Limit key takeaways

Communication efforts should consider the effectiveness of their message on all communication types, whether written or oral, formal or informal, or mandatory or voluntary. The National Association of School Psychologists (NASP) Effective (and Easy) Communications resource guide provides numerous helpful points, outlined in Figure 6-1, that airport operators should consider when communicating to tenants, authorized signatories, and badge holders.

Any message must target an audience with narrow language that addresses their concerns and perspectives. Communication directed at a company will look different than communication for authorized signatories or individuals. A company will care about high-level

compliance issues and the respective fines, whereas an authorized signatory and badge holder need to know their specific responsibilities. A company and an authorized signatory will have a management perspective, whereas an individual will think about their personal responsibility.

Airports should also consider how the audience will interpret the information. The audience will have their own knowledge and awareness of the issue at hand, concerns and expectations, barriers to understanding, and probability to act on the information. To properly tailor communication, the airport must consider a number of things, including the airport culture, the dynamics of the companies that work in the airport, and the turnover of employees.

Similarly, airports should consider the perception of the audience and how the end user will benefit from the communication. The audience may perceive the document or message as an inconvenience, which studies argue prompts resistance to change. Communicators must craft the message with an understanding of how the target audience will interpret it and potentially act upon its content. Clear and concise statements regarding expected actions and the reasons behind the actions will potentially reduce resistance and prompt action. Authorized signatories, for example, have other duties that their company may pressure them to focus on. Cumbersome and obscure documents may foster neglect of responsibilities as opposed to promoting appropriate action.

Similarly, clear and concise language enhances comprehension. Studies have attributed failed organizational changes to the intended audience misunderstanding information presented to them. Communication misunderstandings typically arise due to a lack of clarity in the message. An entity

seeking to drive change must therefore ensure they communicate their message in a comprehensible way. Clear and concise statements simplify matters and reduce the potential for misunderstanding that occurs when a matter is overly complicated. Additionally, publicly available information reduces the risk of miscommunication by providing an easily accessible resource for individuals to reference as needed.

The message should provide the audience with a clear objective that states a main point at the outset and includes specific suggested actions. Active language and the appropriate level of technical content will also assist the reader in interpreting the communication as intended by the writer. The communication should include a clear call to action so that the audience knows their responsibility.

Finally, airport operators should include no more than two or three key takeaways in each communication. The NASP notes that most people only remember two or three points in any communication. Overwhelming a person with too much information risks that the most crucial information will not resonate.

6.2 Key Communication Considerations

- Airports that make rules and regulations, accountability procedures, and security awareness information readily available have consistently low unaccountability percentages.
- All communication efforts must consider the objective of the message and the intended audience. The message must use clear and concise language that is relevant to the audience's understanding of the issue.
- Communication efforts can drive change where tenants have poor management practices in place.
- Effective communication strategies can supplement other control initiatives.

6.3 Potential Communication Issues

Publicly provided information should not contain SSI. Wide dissemination of SSI is not required to achieve this policy option's goal. Information protected by SSI regulations "would be detrimental to transportation security" if released publicly (49 CFR § 1520). Airports can provide SSI through appropriate, protected channels if necessary, and only to persons with a need to know. For example, information about audit techniques and requirements is not necessary for dissemination beyond those individuals involved in the audit process. Conversely, the information provided here relating to high-level public concepts, airport specific rules, and penalties is not SSI and can be freely shared.

6.4 Communication Processes, Practices, and Strategies to Consider

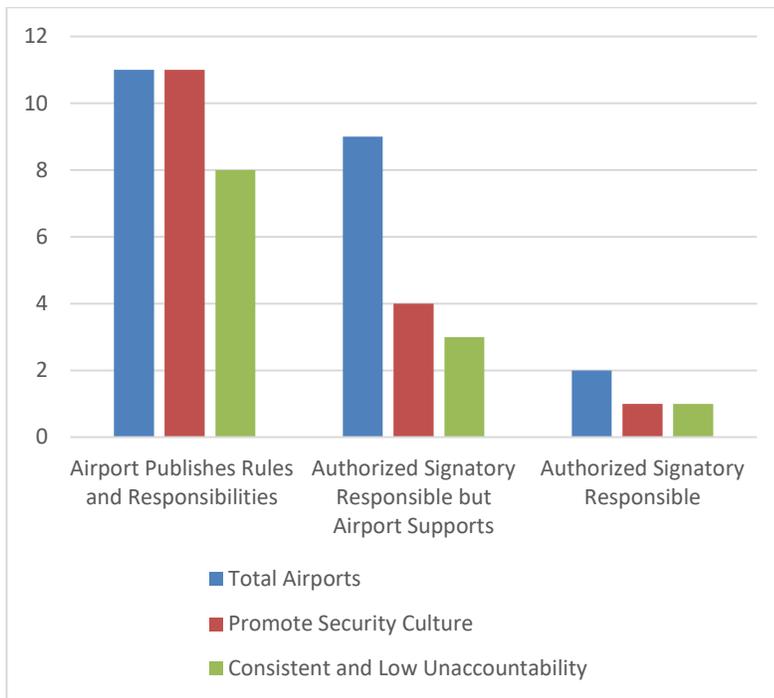
6.4.1 Publicly Available Information

Make rules, penalties, and policies readily accessible to companies, authorized signatories, and badge holders.

Publishing rules, penalties, and policies in an accessible place for companies, authorized signatories, and badge holders can improve accountability. Airports can provide pamphlets or small handbooks in their

badging office, post the information online, or post it on a secure internal network. These policy options ensure that the proper stakeholder has access to relevant information.

Figure 6-2. Public Information and Security Culture in Relation to Accountability



Often, authorized signatories or badge holders report they do not know their responsibility when a badge is lost or access is no longer needed. In some cases, these individuals may not know where to get information, while in other cases the information is not accessible. If posted publicly, the airport can, at a minimum, point to the public information to educate stakeholders or counter the defense of ignorance.

Figure 6-2 illustrates the different accountability rates between airports that publish rules and responsibilities, airports that support the authorized signatory efforts, and airports where the authorized signatory has sole responsibility.

Eight of the 11 airports that published rules and responsibilities and made them readily available for the community reported consistently low unaccountability. Airports that did not publish information and relied on the authorized signatory to communicate rules and responsibilities had lower success rates.

Providing information publicly allows members of the community to access that information on an as-needed basis. It is reasonable to assume that an authorized signatory or badge holder may check publicly available information to verify what their responsibilities are when a situation arises before seeking another source of information.

Advantages:

- **Minimal resources required.** Publishing information publicly may require upfront effort, but once public, the airport will have minimal maintenance issues to consider. Publishing information on a publicly accessible internet site will offer the least resource-intensive option for airport operators, and airport operators can check how often the community views the information.
- **Continuous education.** Publishing information offers an easy way to provide continuous education on rules and responsibilities. Stakeholders will have the option to review the documentation as needed and make appropriate decisions to mitigate the situations they may face.

Alternatives:

- **Training.** New and recurrent training provides information regarding rules, penalties, and policies. The airport may tailor its training to add more in-depth coverage of badge holder responsibilities and penalties.
- **Require authorized signatories to increase communication.** Authorized signatories provide badge holders with information regarding rules, penalties, and policies as they deem necessary. In accordance with regulation, an airport operator may leave the authorized signatory with sole discretion to manage their authorized signatory population as they see fit. This may work at an airport with strong authorized signatories. An airport with high turnover may need to provide a higher level of support to authorized signatories.

6.4.2 Outreach Campaigns**Engage stakeholders through outreach campaigns to strengthen the airport's security culture.**

When communicating, it is important to tailor the message directly to the target audience. For example, specific audiences will have different concerns, perspectives, and levels of knowledge and awareness of each issue. These nuances are likely to be overlooked when addressing broader audiences. Outreach campaigns offer a supplemental opportunity to engage stakeholders, foster a strong security culture, and build security awareness. An outreach effort may fit into a pre-existing security awareness program that the airport has in place. The airport can also focus the outreach campaign on a specific objective that they believe needs attention. The outreach campaign may target a niche population within the stakeholder group and include two or three key takeaways for that audience.

The outreach campaign may include:

- Recognizing strong performing companies at airport manager meetings
- Having badging office staff remind airport badge holders and authorized signatories of the importance of their role in securing the airport
- Placing posters in areas frequented by badge holders that promote vigilance and remind stakeholders of their duties
- Emails to authorized signatories or badge holders with accountability messages
- Security awareness messages in stakeholder newsletters

A Category I airport recently began distributing a brochure to enhance the community's vigilance regarding responsibilities (see Appendix B.) The document is available in the badging office and can easily be distributed at tenant meetings or be provided to authorized signatories for distribution to their badged populations. This document covers all badge holder responsibilities. An airport may alternatively consider a shorter one-pager or poster that focuses exclusively on accountability (see Appendix C.)

Advantages:

- **Outreach campaigns enable airports to target specific audiences with a message.** Not all companies, authorized signatories, or badge holders will need to hear every message. An airport

can address specific issues with targeted outreach efforts designed for a select group(s). Constructing group-specific messages helps ensure that the intended audience knows the information is for them. Targeted messaging also helps avoid loss of audience attention due to spamming.

- **Publishing information offers an easy way to provide continuous education on rules and responsibilities.** Stakeholders will have the option to review the documentation as needed and make appropriate decisions to mitigate the situations they may face.

Alternative:

- **Authorized signatories provide badge holders with rule, penalty, and policy information as they deem necessary.** In accordance with regulations, an airport operator may leave the authorized signatory with sole discretion to manage their badged population as they see fit. This may work at an airport with strong authorized signatories. An airport with high turnover may need to support these authorized signatories.

6.4.3 Authorized Signatory Reference Guide

Provide authorized signatories access to a reference guide.

An authorized signatory reference guide can provide detailed information to assist authorized signatories in managing their badged population. The document should provide in-depth information in a user-friendly manner to assist the authorized signatory in making decisions.

The reference guide can summarize the instructions provided to the authorized signatory during their initial and recurrent training. This may include recommendations for managing badge holder lists and facilitating badge deactivation and return in a timely manner.

Airport operators may provide hard copies of the reference guide in the badging office, post it to a secured internal website, or provide a copy through their IDMS. Because this type of document may include SSI, appropriate measures should be taken to ensure that dissemination is limited to only those with a need to know the information.

Advantages:

- **Publishing information may require upfront effort, but once available the airport will have minimal maintenance issues to consider.** Publishing information on a secured internal site offers the least resource intensive option for airport operators, and airport operators can check how often the community views the information.
- **Publishing information offers an easy way to provide continuous education on rules and responsibilities.** Stakeholders will have the option to review the documentation as needed and make appropriate decisions to mitigate the situations they may face.

Alternatives:

- **Additional training strategies to educate the authorized signatory.** An airport can implement other training strategies, as discussed in Section 5. These include peer-to-peer training or personal meetings with trusted agents.

- **Authorized signatories meet with trusted agents to discuss responsibilities and management practices.** An airport operator can sit down with an authorized signatory and address the issues that specific authorized signatory has in managing their badged population.
- **Enforcement action against the authorized signatory.** As further discussed in Section 7, an airport may impose monetary or non-monetary penalties on the authorized signatory. Non-monetary penalties may include required training or suspension of the authorized signatory's ability to sign applications and renewals.

6.4.4 Authorized Signatory Responsibility Summary Sheet

Provide authorized signatories with a responsibility summary sheet reminding them of their ID media accountability responsibilities and where to receive assistance.

Airports may consider providing authorized signatories with a summary sheet that provides instructions and information regarding their accountability responsibilities. Many airport operators reported that their authorized signatories do not pay adequate attention to their duties, and frequently claim ignorance when asked why they have neglected a duty. This policy option will assist airport operators whose authorized signatories fail to effectively manage their responsibilities, or airports with high authorized signatory turnover.

The sheet should include concise reminders of responsibilities and how-to statements, not in-depth instructions or regulatory language. The sheet should not exceed one page, as this is not intended to provide detailed information to the authorized signatory. The document should provide a quick reference to remind the authorized signatory of their duties or assist them in finding additional information.

Advantage:

- **Easy resource to assist authorized signatories in completing their duties.** The authorized signatory can reference the sheet on an as-needed basis to remind them of their responsibilities, or to assist in identifying an appropriate resource to address a problem.

Alternative:

- **Offer drop-in office hours for authorized signatories to speak with trusted agents.** This option similarly provides authorized signatories with a resource if they face an issue they do not know how to resolve.

SECTION 7: ENFORCEMENT

7.1 Overview of Enforcement

Airports commonly use penalties and incentives to manage accountability. However, penalties and incentives are most effective when used in combination with a broader enforcement strategy. Airport operators use various penalty and incentive processes, practices, and strategy options to control ID media. These policy options vary in form, severity, application, targeted audience, and frequency of use. Issues of airport culture and political feasibility may enhance or limit an airport's ability to impose monetary or non-monetary penalties. Similarly, some local laws or ordinances may require legislative action by city councils or boards before imposing penalties. Creative airports will find penalty options that provide flexibility and support the airport culture while avoiding political resistance or bureaucratic barriers.

Understanding how a company, tenant, or individual badge holder will react to penalties or incentives will assist the airport operator in determining whether they should change their penalty policies or try alternative policy options to support their control efforts. Airport operators may use classical deterrence theory principles to assess whether they have effective penalties in place or whether a proposed alternative penalty option could reduce unaccountability percentages.

Classical deterrence theory contends that the introduction of a penalty will reduce a behavior. The effectiveness of a penalty depends on the certainty, severity, and swiftness of enforcement. The target audience must understand the rule and consequences for not following that rule. According to classical deterrence theory, the targeted actor must understand that the sanction results from the violation of the rule and that the penalty outweighs the benefit of such action. Two examples from the airport interviews illustrate this theory in practice.

First, some of the airports interviewed only fined companies for violations once a year. These airports thought a company would improve their poor ID management practices after receiving a significant penalty. In some instances, these fines did not deter the behavior as companies repeatedly failed to account for their badges, and consequently paid the penalty on a yearly basis. These airports should consider whether the companies appropriately attribute this penalty to their poor badge accountability practices. Second, other airports interviewed reported that their penalties were viewed as the cost of doing business. Therefore, these airports should consider raising the cost of the penalty to increase deterrence.

At an airport, the penalty can focus on the company, the authorized signatory managing its badged population, the individual badge holder, or any combination of the three. Airports generally chose to penalize the individual badge holder or the company. Some airports have had success targeting all three groups.

In establishing penalties, the airport must consider whether it can manage enforcement of the penalty, whether the punishment deters the targeted audience from the behavior, and whether the airport can enforce the penalty within a reasonable timeframe for proper attribution to the targeted behavior.

Penalties may cause discontent within the community. As discussed in Section 6, airport operators should consider outreach and education strategies to ensure the stakeholders know the airport priorities, their responsibilities, and the consequences for failing to meet those responsibilities.

An airport operator attempting to change poor behavior should consistently enforce their penalty structure. Operant conditioning, a learning process theory, hypothesizes that establishing a new behavior requires continuous consistent enforcement. Once established, an airport can adopt partial enforcement of the penalty, but must ensure that poor practices do not return as enforcement reduces. Punishment can suppress behavior, but that behavior often returns when enforcement ceases or is mitigated.

In some cases, fines can undermine the sense of ethical obligation. Behavioral economic studies in other industries have found that fines help individuals rationalize behavior. The fine, in effect, creates a mindset that if you know the penalty, you know the boundary and can accept the penalty for noncompliance. Tenants or badge holders may view the fine as the cost of doing business. Put another way, the fine can represent the cost of not accounting for ID media. A tenant may decide the fine justifies noncompliance, or the badge holder may find it easier to pay the fine than to find their lost badge. In these circumstances, an airport may adopt a more aggressive policy of recovery, even after the badge expires and is no longer technically an item subject to audit accountability.

Airports must also consider that people adapt to punishments, causing penalties to potentially lose effectiveness. To mitigate this concern, an airport may need to increase the severity of the penalty or alter enforcement in a manner that keeps the targeted audience aware and incentivized to comply. If an airport cannot change monetary fines, they may consider non-monetary penalties, such as additional training or shortening a company's badge renewal period. An airport may also alter its enforcement strategy, potentially levying fines at various times or prioritizing different accountability failures.

In developing or assessing penalty options, airports must appreciate that penalties can suppress targeted behaviors, but do not teach proper behavior. Penalties will tell the targeted audience to return, to not lose, or to properly account for ID media; but not how to return it, strategies to not lose it, or how to better manage ID media populations. An airport should consider how their penalty policies fit into their broader control strategies. Enforcement strategies and reinforcement practices should complement one another.

Airport operators must properly document processes, outreach, and failures to comply to support penalties. Tenants or badge holders may challenge a penalty and argue they did not know of their responsibility or that they did not violate a rule. Proper documentation of training where badge accountability was covered, documentation that the badging office spoke with the entity or person regarding rules and responsibilities, and a log of violations with pertinent facts will assist the airport in justifying the penalty.

7.2 Key Enforcement Considerations

- Enforcement policies varied consistently among the airports interviewed regardless of airport size.
- Airports should develop a comprehensive enforcement strategy that encompasses penalties tailored to the behaviors the airport seeks to deter. Auditing can assist in the planning and execution of this strategy.
- Airports that face restrictions on their ability to fine or increase fines should consider alternative non-monetary penalties that will drive process change for companies and their authorized signatories, or build security awareness in the badge holder community.

- Higher value penalties do not, by themselves, result in lower unaccountability or consistent accountability percentages.
- Airports that hold companies liable for returning ID media have lower unaccountability rates. This is accomplished through monetary fines significant enough to draw the attention of company leadership, or through non-monetary penalties that affect the company's ability to conduct business in the airport. Alternatively, some airports achieved success by focusing non-monetary enforcement on specific authorized signatories.
- Two airports with active enforcement of lower value monetary penalties have strong security awareness initiatives and consistently low unaccountability percentages.

7.3 Potential Enforcement Issues

- **Community and Airport Leadership Support.** Penalties may cause consternation within the airport community. Gauging and managing acceptance among airport stakeholders is critical to the strategy succeeding. Having support of airport leadership will assist in managing the airport community. Airport leadership is more likely to back an enforcement strategy that matches the airport's strategic priorities.
- **Managing strategies.** Execution of enforcement strategies requires significant airport resources. The trusted agent must first analyze relevant auditing data or observe the concerning behavior, and document wrongdoing. The airport must then determine whether to impose a monetary or non-monetary penalty to deter similar non-compliance.

If the airport chooses to impose a monetary penalty, it must find a method to ensure collection; if it chooses a non-monetary penalty, it must find a method of fulfillment. For example, non-monetary penalties may include training classes, changed renewal periods, or suspending or revoking access privileges. Each of these methods require the expenditure of additional resources to ensure compliance.

No matter what penalty it chooses to impose, the airport must be prepared to defend that penalty if challenged. Accordingly, an airport must consider whether it can properly execute its chosen enforcement strategy to deter the concerning behavior.

- **Local Restrictions.** An airport's ability to impose or change the value of monetary penalties may be restricted by local laws or administrative processes. Getting political support to change a law can be difficult and time consuming. Airports may choose non-monetary penalties to avoid these challenges.

7.4 Enforcement Issues Processes, Procedures, and Strategies to Consider

The following process, procedure, and strategy options offer ways for an airport to incorporate an enforcement plan into its culture to enhance controls and badge holder accountability.

7.4.1 Diverse Penalties

Implement a penalty structure that includes a combination of fines and non-monetary penalties directed at companies, authorized signatories, and badge holders.

Airport operators may consider a diverse penalty structure that targets all parties who have a responsibility in ID media accountability. This policy option seeks to deter behavior at all levels of the process in a manner that causes change across the board. An airport may implement a series of monetary and non-monetary penalties that target the company and its authorized signatories, while also ensuring badge holders comply with their responsibilities. For example, an airport can fine a company for total unaccounted-for ID media at the end of a specified time period, require the company to develop a compliance plan for auditing failures, suspend an authorized signatory's access to the badging office for poor management practices, and impose a fine when an individual seeks to replace a lost badge.

As part of a robust enforcement regime, an airport should review data about its penalty enforcement to identify behavioral trends. This will allow the airport to intelligently adjust penalty and enforcement policies. The airport may choose to enhance the frequency of enforcement, or reduce the use of a specific penalty in favor of another measure that targets a new problem area. Compared to fines, non-monetary penalties may offer an easier option to change the enforcement approach.

Airports should consider the impact of different enforcement actions when developing a diverse penalty structure. Company-centric penalties should be designed to promote improvement of poor management practices. This requires a penalty that is not so small that it is potentially dismissed as the cost of doing business, nor should it be excessive, which may prompt the company to decide there is no point in expending resources to try to comply. Authorized signatory penalties should seek to ensure vigilance. An airport can fine authorized signatories for failing to manage their badge holders or impose non-monetary penalties designed to improve management practices. Finally, monetary penalties for individual badge holders tend to be smaller and may be easier for a company to cover on behalf of the badge holder if they choose to do so. A non-monetary penalty for an individual badge holder may seek to improve their knowledge of their responsibilities.

Diverse and active enforcement policies alone did not result in the strongest ID media control programs. The strongest-performing airports with diverse and active enforcement strategies also used auditing practices to discover issue areas and mitigate as necessary, strong trusted agent practices, and some engagement with authorized signatories or companies. Of note, these airports generally based their renewal periods on factors other than control concerns.

Airport operators choosing a policy of aggressive enforcement with fines and penalties should use lessons learned from their audits and other ID media control policies to drive enforcement strategies.

This strategy will impose an administrative burden on the airport to manage the complex penalty process. The airport operator will have to assess and collect fines, ensure enforcement of non-monetary penalties, and adjudicate penalty appeals.

Advantages:

- **This robust penalty structure holds all members of the airport community accountable for their actions.** An airport operator that uses this penalty strategy can target the root cause of an issue. If, for example, the airport only imposed fines on the company for the loss of ID media, the airport would have to rely on the company to drive change at the badge holder level where the issue may originate. With multiple penalty options, the airport can assess the cause of the problem and enforce accordingly.
- **Robust penalty structures can keep the airport community on its toes.** With multiple penalty options, the airport can prioritize the behavior it wants to target for enforcement, such as poor management practices, bulk return of ID media, or lack of vigilance on the part of badge holders.

Alternative:

- **An airport operator can implement a less complex penalty structure and achieve strong unaccountability percentages.** The airport can target one stakeholder and impose a fine or non-monetary penalty of their choosing. For example, the airport can fine an individual for losing their badge. This option will require less burden to administer the penalty. An airport that chooses a simplified enforcement policy should consider strong trusted agent, security awareness, and authorized signatory or company policies.

7.4.2 Non-Monetary Penalties**Implement a non-monetary penalty system for companies with consistently high unreturned badge percentages.**

Non-monetary penalties that target companies with consistently high unaccountability percentages may improve an airport's overall control of its ID media program. Many airports that impose non-monetary penalties for companies with consistently high unaccountability percentages tend to have consistent audits throughout the year with unaccountability levels that are safely under reissuance levels.

Non-monetary penalties for problem companies can include:

- Suspending issuance or renewal for failing to manage accountability
- Suspending or limiting privileges of authorized signatories for companies with poor accountability records
- Shortening a company's renewal period
- Requiring a company to submit an ID media accountability action plan
- Requiring additional training for company personnel and authorized signatories

Many of these measures will impose a significant burden on the company and authorized signatory. These policies therefore require airport leadership support to address push-back, potentially from powerful tenants.

Non-monetary penalties will potentially require additional administrative support to enforce the measure. The airport may have to teach a training course, have an additional meeting, and review an action plan, among other things.

Airports may consider targeting companies whose unaccountability exceeds three or five percent with non-monetary penalties. The three percent threshold will require the company to stay vigilant and prevent mistakes. Additionally, airports may target companies that show poor management techniques. Airports can base the assessment on audits, or note when a company deactivates numerous badges at one time.

Advantages:

- **Non-monetary penalties can bridge the gap between enforcement for bad behaviors and reinforcement of good behaviors.** Non-monetary penalties punish bad behavior by imposing a burden on the offender, but reinforces good behavior by requiring some positive action to address the failure.
- **Implementation of and changes to non-monetary penalties often require fewer, simpler, or more flexible administrative processes.** Many airports face restrictions from local laws and ordinances on monetary penalty values, or have numerous administrative hoops to manage a monetary penalty. An airport may have the ability to implement some non-monetary strategies to avoid these barriers.

Alternative:

- **An airport can impose monetary penalties.** An airport may choose to impose *only* monetary penalties to deter behavior. Monetary penalties, when paired with other non-enforcement options, can affect accountability. Some monetary penalties may require less of a burden on the airport to manage.

7.4.3 Threshold for Company Penalties

Penalize companies when their unaccountability rates exceed a percentage threshold.

An airport may decide to impose monetary and non-monetary penalties on a company when their companywide unaccountability percentages reach a predetermined threshold. Airport operators that implement this strategy set their own thresholds, but five percent is the most frequently used. One airport interviewed with low and consistent unaccountability suspends a company's access to the badging office and fines the company \$100 for each badge while they exceed the defined threshold. Another airport suspends access to the badging office and requires the tenant to submit an ID media management plan to end the suspension.

This option will require a process or a technology system, such as an IDMS, to provide a periodic picture of a company's unaccountability percentage.

This option may require airport leadership support as it may cause worry among the airport tenant community. A company may quickly find itself exceeding a threshold because of an event out of their control, such as unexpected high turnover.

Advantages:

- **Percentage threshold penalties for companies provide a generally straightforward process for airport operators to manage.** The airport must assess its audit findings and impose the penalties accordingly.

Alternatives:

- **An airport can penalize companies for the total number of unreturned badges at set periods.** Airport operators that do not have a technology solution to support the threshold strategy may find it easier to manage penalties based on the total number of unreturned badges. Tenants may prefer this option as they would potentially have time to mitigate issues before receiving a fine.

7.4.4 Graduated Penalty Structure

Implement a graduated penalty structure that increases based on the level of noncompliance.

Graduated penalties increase based on continued noncompliance. If a company, authorized signatory, or badge holder continues to neglect the same responsibility, they will receive an increasingly severe penalty after each infraction. The graduated penalty structure can be monetary or non-monetary in nature, or a combination of both.

Of the airports interviewed, those with graduated penalty structures had consistent accountability percentages. The lowest unaccountability rates of the airports with graduated penalty structures had higher level penalties and other practices, such as proactive auditing strategies, to assist with accountability and control.

Graduated penalty structures may cause an added burden on the airport to manage proper enforcement and escalation of the measures.

An airport should assess how its tenants respond to the enforcement actions when considering a graduated enforcement structure.

Advantage:

- **Graduated penalty structures enhance deterrence for repeat offenders.** This strategy seeks to mitigate the “cost of doing business” mentality. With each subsequent penalty, the offender may decide the penalty outweighs the burden of changing the problem behavior.

Alternative:

- **Impose standard penalties for subsequent violations.** Using consistent enforcement measures for violations may reduce the administrative burden on the airport to manage the process, and enable the airport to use resources in other areas.

7.4.5 Penalty Refund

Refund monetary penalty if a company or individual can mitigate unaccountability within a specific period.

An airport may choose to incentivize a company or individual to return ID media after a fine is issued by reimbursing the fine if the badge is returned in a specified amount of time.

One airport interviewed had a practice of fining tenants once a year. If the tenant found an unreturned badge prior to the issuance of the fine, they would not receive a penalty. The airport believed this gave companies more time to find the badge, and they would work harder to get it back.

Similarly, an airport can choose to return a portion of the fine. Some airport operators that target their fines at badge holders will offer a partial refund of the fine if the individual later finds the badge and returns it to the airport.

Advantage:

- **Refunds incentivize the return of ID media.** The penalized party may continue to search for the badge after assessment of a penalty if they know all or a portion of the penalty will be refunded. An airport benefits from having reduced unaccounted-for ID media.

Alternative:

- **The airport can choose to not return fines or reduce penalties if the ID media is later found and returned.** Most airports interviewed for this project adopted this approach. These airports consistently held the strong belief that refunds could incentivize noncompliance.

7.4.6 Police Reports

File a police report for non-returned badges.

Airports may consider filing police reports when a badge holder leaves their employment and does not return the badge to the airport or their former company. This may work well for airport operators that focus control strategies on badge holders. The strategy may also deter people from falsifying explanations for lost badges.

The airport may choose to file police reports for all non-returned badges or as a mitigation measure only when unaccountability rates begin to rise. Similarly, filing police reports periodically or on an as-needed basis may raise awareness within the badge holder community that the airport prioritizes badge return. For many airports, this approach may require cooperation from external police agencies.

Advantage:

- **Individuals may return their badge to avoid having a police report filed.** This strategy may increase vigilance within the airport community if they know the airport will take such an action.

Alternative:

- **Penalize sponsoring authorized signatories or companies for non-return of ID media.** Airports may find it easier to follow a traditional enforcement strategy and impose the burden on the company or sponsoring authorized signatory.

7.4.7 Construction Contracts

Include fees for unreturned badges in construction contracts.

An airport can include language in a construction contract that requires the contractor to pay a fee or forfeit a portion of the contract amount for unreturned badges. Airport operators that have implemented this requirement have found that contractors pay more attention to collecting and returning badges at the conclusion of a project.

Local laws or airport policies may present barriers to imposing such contractual language.

Advantage:

- **Contractor knows the issue is important.** Putting the issue in the construction contract lets the contractor know the importance of the issue and compels good management before issues arise.

Alternative:

- **Set expiration dates for end of contract.** Airport operators may choose this option if they cannot impose a fee or withhold a portion of the contract.

7.4.8 Fixed Base Operators

Include unreturned badge fees in the Fixed Base Operator (FBO) or individual hangar lease agreements.

Airport operators that have difficulty with FBOs have included fees in the FBO or individual hangar lease agreements. Similar to construction contracts, the additional contractual language has influenced FBOs or individuals leasing hangar space to pay more attention to badge accountability.

Advantage:

- **Places burden on FBO or individual.** The stakeholder must properly manage the ID media to avoid additional fees.

Alternative:

- **Impose standard monetary penalties.** An airport that cannot change contractual language may choose to rely on monetary penalties. The penalty must impose a significant enough burden on the FBO or individual to increase vigilance.

7.4.9 Badge Return Moratorium

Host a Badge Return Moratorium to mitigate a rising unaccountability rate.

An airport operator may consider offering a week- or month-long enforcement moratorium to encourage authorized signatories to return outstanding badges. Many authorized signatories hold onto badges and return them at one time. These individuals may hold onto them longer than necessary to avoid the enforcement they know will follow. A moratorium, tailored to the airport's enforcement strategy, may assist the airport operator in quickly collecting many badges.

As an illustration of this strategy’s effectiveness, the City of Sydney, Australia instituted a moratorium on library fines and received triple the number of unreturned books back within a seven-month period than they had received in the previous year. Sydney found their staff was spending too much time enforcing unreturned book fines rather than delivering library services. They believed the fines discouraged library members from returning their overdue books. The library alternatively suspended library memberships until books were returned. As a result of these initiatives, the City of Sydney concluded the measures “encourage[d] positive community responsibility.”

An airport near a reissuance or reporting threshold may consider this process to boost the number of returned badges and reduce the airport’s overall unaccountability percentage. However, this measure may also create an expectation within the community that penalties can be avoided by waiting for the airport to grant a moratorium.

Advantage:

- **Easy for the airport to manage.** This strategy presents a low-risk, high-reward option for airport operators. Authorized signatories may take advantage of the opportunity and help the airport improve its unaccountability percentage.

Alternative:

- **Implement an enforcement action that targets bulk return.** An airport can impose stiffer penalties for bulk return of badges in an attempt to prevent the issue from occurring in the first place.

SECTION 8: BADGING OFFICE AND TRUSTED AGENTS

8.1 Overview of Badging Office and Trusted Agents

Airport badging offices and trusted agents play a key role in managing ID media control practices. The badging office staff and trusted agents must understand the relationship between the policies they implement and their effect on control. Vigilance in completing badging office duties and clarity in the messages that the office communicates to stakeholders will present a strong security culture to the community that may inspire others to uphold their responsibilities. Airports should be mindful that in many cases, the only human communication link between the airport and the badge holder is the trusted agent or badging office staff member. The communication they provide on the importance of accountability should not be underestimated.

Airports must consider the dynamic of their human resources in planning operational policies. The ratio of trusted agents and badging office staff to the badged population varies significantly between airports. For example, one Category X airport interviewed had more than 15 staff members and five trusted agents, whereas another Category X airport with a similar population had only three staff members and three trusted agents. These airports had wide-ranging distributions of responsibilities among trusted agents and staff, with trusted agents overseeing ID media processing, based on their available resources. Some airports do not have permanent ID media staff; airport operations staff rotate through the responsibility. Other airports do not have a dedicated badging office, and may only offer processing once per month.

8.2 Key Badging Office and Trusted Agent Considerations

- Policies and procedures, team briefings, and other forms of engagement help badging office staff and trusted agents remain vigilant and consistent in their efforts to control ID media.
- Airport operators with strong security cultures have effective badging office and trusted agent practices in place.

8.3 Potential Badging Office and Trusted Agent Issues

- **Vigilance.** Badging office staff may exhibit apathy due to the repetitive nature of their job. This may cause errors in the completion of important processes and procedures that affect control of ID media.
- **Transient trusted agents and badging office staff.** Not all trusted agents work in the badging office every day, and some smaller airports transfer staff in and out of ID media roles. Without a complete understanding of daily processes and procedures, these individuals may miss key elements necessary to effectively control ID media.

8.4 Badging Office and Trusted Agent Processes, Procedures, and Strategies to Consider

8.4.1 Expired Badges

Pursue unreturned or lost badges with the same vigor whether it is expired or unexpired.

Airport operators that reported pursuing all issued badges with the same policies, whether unexpired or expired, reported consistently low unaccountability. Airport operators interviewed noted that tenants and authorized signatories knew whether an airport would continue pursuing the unreturned or lost badges based on the local policy. Where the airport indicated it would not pursue such media, there was concern that this would send the wrong message to companies about the importance of accountability.

One airport reported that it kept badges on a tenant's unaccountability list for one year after expiration, and therefore continually included them in enforcement decisions against the tenant. This airport provided TSA with a separate unaccountability report after required audits that included only non-expired badges, as mandated by TSA.

Advantage:

- **Security Awareness.** The airport community will know that the airport prioritizes badge accountability and that the passage of time will not mitigate their unaccountable percentage.

Alternative:

- **Focus on unexpired badges.** An airport can choose to focus on unexpired badges.

8.4.2 Policies and Procedures

Document policies and procedures for trusted agents and badging office staff.

Written policies and procedures will assist badging offices in ensuring consistency of operations. Our research shows that airports with written policies and procedures for their trusted agents and badging office had lower unaccountability percentages. These written policies and procedures included practices for badge issuance, renewal, and return. This can include processes that provide checks and balances to ensure accurate data collection and record keeping.

Many airport operators interviewed had unwritten policies and procedures for trusted agents and staff, or no policies and procedures at all. These airports may send their trusted agents and staff to outside training, train them in-house, train them on the job, or provide no training at all. The absence of written policies and guidance leaves room for error and the development of unproductive practices.

Advantage:

- **Consistent operations.** Written policies and procedures will assist badging offices in performing both routine and complex tasks. Additionally, written policies assist airports in training new staff and trusted agents.

Alternative:

- **Routine staff briefings.** Routine staff briefings can strengthen consistency and adherence to policies and procedures. Additionally, the meetings will ensure the staff are on the same page and up to date on processing information.

Create detailed instruction sheets for badging office employees to reference.

A detailed instruction sheet will provide badging office employees with a tool to assist them in completing tasks, and remind them to remain vigilant. The document can serve as a resource for staff to ensure they follow protocol. Permanent staff will benefit from the document as a reminder to remain vigilant, while temporary staff will have an aid to assist them in completing a task that is not their permanent duty.

Advantage:

- **Easy resource to increase vigilance.** Providing a detailed instruction sheet does not require much resource investment on the part of the airport. Once initially put together, the airport only needs to amend the document as processes change.

Alternative:

- **Training.** Provide training for all badging office staff. Airports can provide this training in-house or send staff to a third-party provider.

8.4.3 Situational Awareness

Engage badging office employees to show them why their role is important and how it affects airport security.

Airport operators may consider having internal badging office meetings to show the staff why their work is important. Badging office staff often sit in a processing center in the public area of the airport and may not get to see how the airport operates and why their work is important.

An airport interviewed began closing the badging office once a month for a half-day meeting. Part of the meeting is used to show the staff the impact their work has on the airport community. Sometimes the meeting consists of briefings discussing security awareness topics and ID media best practices. The half day is also used for field trips that give staff the opportunity to learn about other airport jobs or ongoing projects.

Advantage:

- **Security awareness.** Badging office staff may lack firsthand observations of why their work matters. This team building exercise will teach them how their work enhances security and why they must remain vigilant in completing their duties.

Alternative:

- **Routine staff briefings.** Routine staff briefings can strengthen consistency and adherence to policies and procedures. Additionally, the meetings will ensure the staff are on the same page and up to date on processing information.

8.4.4 Internal Audit

Audit airport ID media control practices.

Airport operators may consider auditing ID media control practices to identify areas for improvement. Regulation requires that airports audit their badge issuance processes, but there are also other duties that fall under the badging office's responsibilities. Control of unissued badging supplies, access to badging office equipment, deactivating badges, or proper processing of returned badges all merit attention. Implementing an inspection or audit process for these controls will serve as a check on the process and potentially improve vigilance. The audit process may offer insights into policies or procedures that need improvement.

Advantage:

- **Check and balance.** An internal audit will allow the badging office to check its work and assess the value of their processes, practices, or strategies.

Alternative:

- **Routine staff briefings.** Routine staff briefings can strengthen consistency and adherence to policies and procedures. Additionally, the meetings will ensure the staff are on the same page and up to date on processing information.

8.4.5 Review Need for Secured Area Access

Require tenants to review and attest to continued need for secured area access.

The badging office may consider asking tenants to periodically review and confirm their continued need for secured area access. This revalidation process would require the tenant to review their current list of badge holders and state that each individual listed still works for the company and requires continued access.

This process may result in the company better managing their badged population. By revalidating the need for access, the authorized signatory is checking on the status of that badge holder. This may result in the deactivation of access privileges that were overlooked, or the return of badges that the authorized signatory has failed to return.

Advantage:

- **Authorized signatory management check.** This process will enable the badging office to check in with authorized signatories between audits and renewal requests.

Alternative:

- **Annual and partial audit.** The airport reviews the accuracy of authorized signatory record-keeping through the annual and partial-audit processes.

Deactivate ID media that remain unused after a specified amount of time.

Airport operators with automated access control systems capable of monitoring and reporting badge use may consider deactivating badges that remain unused for a specific amount of time. The airport can

provide a list of unused media to the tenant, and state that the airport will terminate the badges if the tenant does not request continued access for that individual. In airports where badges are related to an ACS, the airport may require that they are swiped in an ACS reader within a certain period (for example, 60 or 90 days). The automated ACS can generate badge-usage audit reports. Where that ACS is tied to biometrics, the act of reading the badge demonstrates compelling evidence that it is in the possession of the assigned owner.

Advantage:

- **Reduce exposure to misuse of ID media.** Require the authorized signatories to review their record keeping to confirm that they know the status of each badge holder.

Alternative:

- **Review access needs.** Require authorized signatories to review and confirm the access needs of their badged population.

SECTION 9: AUDITING

9.1 Overview of Auditing

Auditing remains a focal point for ID media accountability at airports. The need for an audit, in general, derives from outside stakeholder pressures for accountability. The Gore Commission Report and resulting FAA regulation introduced accountability to badge issuance in 2001. Congress continues to believe that outstanding badges represent a threat to aviation security. The DHS IG agrees with this point, and has reported issues with TSA oversight and airport accountability of ID media. As a result, TSA implemented new compliance measures to test airport controls, and issued a new ASP NA in 2019.

Although the ASP NA offers three auditing options, it does impose strict requirements regarding how to complete annual and partial audits. Still, auditing strategies will vary among airports for the same reasons that accountability policies will also differ. Functions of an audit will therefore depend on the organization and its business model. An audit strategy must consider the organization, strategies, resources, and the mix of tenant organizations at the airport.

The audit offers an opportunity to highlight potential areas for improvement and facilitate changes within the organization. A well designed and executed audit will provide points of analysis regarding badge accountability and control practices. An audit strategy sets the direction, timing, and scope of an audit. Although the specifics of an audit will vary, the following key principles will assist the airport in conducting an audit that provides effective information:

- Objective
- Strategy
- Scope
- Measurable goals

The audit strategy must include clear statements of the meaning, significance, and intention of the audit. The focus of the audit can vary based on the objective. The airport may focus on strengths or weaknesses of the ID media program. Similarly, the airport may choose to conduct a longer term, multi-step audit that provides more in-depth analysis, a shorter-term audit for immediate results, or a combination of both.

Airports should plan and conduct audits in a manner where the benefits outweigh the costs for their organization and ID media program. An airport must understand what they want to achieve with the audit and plan accordingly. An intensive audit can assist the airport in planning and implementing new processes, practices, and strategies. The data provided by the audit will assist in analyzing issues, developing mitigation measures, and setting new parameters to measure effectiveness.

An airport may also want to use the audit as a status check for itself and its tenants. An airport in this circumstance can define its criteria and set an audit strategy to complete an assessment. Alternatively, an airport may have limited resources to dedicate to ID media control, and therefore may choose a less resource-intensive option that creates awareness regarding the quality of the ID media program.

As discussed in the penalty section, an airport should consider additional audits when findings indicate that a tenant is noncompliant. The airport can design the audit strategy around the compliance failures to assist the tenant in improving their ID media program.

The TSA Aviation Security Advisory Committee (ASAC) Working Group on Airport Access Control Final Report from April 2015 includes a discussion of internal controls for auditing credentials as part of a risk management system to mitigate threats associated with access control. The ASAC offered strong auditing and control recommendations to enhance accountability. The list of recommendations is included in Appendix D.

PACS and automated data analytic systems, such as IDMS, can assist an airport in standardizing an audit and gathering necessary data. These systems can run control tests and track progress. The airport can program specific audit requirements into the IDMS. The system will then generate and email audit letters automatically and monitor audit responses. Of note, an airport should consider data security and quality control when using any automated data system. Section 11 further discusses PACS and IDMS.

9.2 Key Auditing Considerations

- The data collected did not show that auditing practices alone can impact badge accountability. Moreover, successful programs adopted a variety of auditing options.
- Some successful airports use their audit findings to drive enforcement activities, policy change considerations, auditing strategies, and stakeholder engagement.
- In addition to audits that meet TSA standards, airports can employ alternative audits to assist in ID media control. For example, these audits may use tenant work schedules or parking permit lists. The airport can conduct these audits on their own or require a tenant to conduct the audit and report the results.

9.3 Potential Auditing Issues

- **Resource intensive.** ID media auditing processes, practices, and strategies require the airport to use significant resources. The process is time consuming, so the airport may consider using technology solutions to assist. Airports therefore may consider maximizing the benefit they receive from the audit practice because of the resources they must dedicate to meeting the regulatory requirement.
- **Tenant record keeping.** Poor tenant record-keeping increases the complexity of an audit for airport operators. Training and communication outreach strategies can assist airports in improving their tenants' and authorized signatories' recording practices.

9.1 Auditing Processes, Procedures, and Strategies to Consider

9.1.1 Badge Control Through Auditing

Implement an audit strategy that leads the airport's decision-making for ID media control efforts.

An airport can use its audit process to manage and plan ID media program accountability and control. The audit process provides insights into airport tenants' accountability practices and how airport control strategies impact accountability. Airports adopting a proactive auditing strategy can tailor the audit to learn specific information, and then use that information to improve policies and practices.

To succeed, the airport must tie other processes and procedures to the auditing goal. The audit goal should address a specific issue the airport wants to improve. For example, the airport may want to

reduce bulk badge deactivation, or the airport may choose a security-related goal that does not concern accountability (for example, checking a badge holder's need for a certain level of access).

Auditing can focus on both long-term and short-term objectives. Partial audits can measure progress or identify trends over time. The airport operator should define what they want to learn from each audit and set parameters accordingly.

The airport should engage tenants to discuss audit findings and impose appropriate penalties or remedial measures to address deficiencies.

This auditing policy will involve significant staff resources to plan, execute, and conduct appropriate follow-up.

Advantage:

- **Maximize benefit of audit.** Auditing can inform management decision-making and help shape other measures to enhance accountability. For example, it may inform judgments on the appropriate levels of fines or penalties, or time periods for badge renewal.

Alternative:

- **Baseline audit.** Airports can find ways to simplify the auditing process and reduce the amount of resources required to meet the regulatory requirement. This may benefit airports that have other security concerns that use the airport operator's limited resources.

9.1.2 Baseline Auditing

Implement an auditing strategy that meets only the regulatory baseline.

Airport operators may consider implementing an audit process that solely meets the regulatory baseline. The airport can use the data gathered in this process to understand its position regarding unaccountability and glean trend information. This strategy will benefit airport operators that do not have the staff or resources necessary to enhance their auditing strategy.

Five of the eight airports interviewed that reported baseline auditing strategies had low and consistent unaccountability. These five airports also had badging office policies and procedures, and other checks and balances in place. Other control strategies varied among these five airports, leading to the conclusion that multiple paths to success exist with baseline auditing.

Advantage:

- **Redistribute resources.** Airports may find ways to save resources in completing the audit requirements, and then redistribute those resources to other security concerns requiring attention.

Alternative:

- **Drive ID media decision-making through audit.** Airports can use the audit processes to plan and execute their ID media program processes, practices, and strategies.

9.1.3 Problem Companies

Conduct additional audits for companies that have trouble managing their badged population.

Additional audits for problem companies may force their hand to improve management practices. For example, an airport may impose quarterly audits until the company improves, or the company submits a new management strategy to the airport operator. The company will have an interest in improving its performance to avoid the additional work.

Airports can implement creative auditing strategies in these circumstances because they will occur outside of the TSA-mandated auditing processes. Therefore, the airport can impose a majority of the burden on the company if it chooses. Airports can use things such as access control records or employee parking lists to validate the audit.

Advantage:

- **Attentiveness.** Additional audits will require problem companies to address their management issues directly.

Alternative:

- **Training and Outreach.** Airports can choose to provide additional training for, or outreach to, authorized signatories regarding record keeping and auditing processes.

9.1.4 Badge Accountability Through Auditing

Verify that badge holders possess their credentials by checking access control records.

An airport can establish badge accountability using IDMS and PACS. A swipe of the badge at a PACS terminal will tell the IDMS that it was used. Some PACS can generate badge usage reports independent of an IDMS. An airport can check that information with employee records provided by the tenant.

Accountability validation is enhanced in airports with two-factor authentication capabilities in their PACS, such as a badge and a biometric. In the case of a biometric, the badge swipe at an access point and simultaneous biometric submission will enable the PACS to provide data to an IDMS or generate a report indicating that the badge was used by a person with the same biometric as it was issued. This provides an affirmative audit trail indicating that it is in the possession of its owner. The airport can use this data for a real-time audit of all badge holders across the entire enterprise.

Of course, the use of IDMS and automated PACS are not without cost. These systems require complex integration and continuing data updates to ensure their reliability. IDMS can assist in media accountability, but adopting these systems requires careful planning and thoughtful implementation.

Advantage:

- **Positive ID control.** Using IDMS or PACS ensures airport operators that the badge holder has accessed the secured area within a specified period of time. The identity verification tool ensures that the person swiping the badge is the person that is supposed to have it.

Alternative:

- **Authorized signatory attestation of access needs.** Airports can require that authorized signatories confirm the continued access needs of their badged community.

SECTION 10: LOW UNACCOUNTABILITY TRENDS

The airports interviewed that reported unaccountability below two percent offer evidence of the variety of policies that can achieve strong accountability. These airports include three Category X airports, two Category II airports, and one Category III airport. The ID media programs, although tailored to their individual needs, all have a core feature of strong management practices. Each airport has a well-trained and engaged badging office, and ensures their authorized signatories or companies implement supporting management practices. One airport in this group has significant authorized signatory engagement. Finally, all these airports have some form of written or unwritten policies and procedures for their badging office, and provide training for the staff in those policies and procedures. Table 10-1 displays the results from the interviews of the six airports.

Airports with low unaccountability rates did not report any of their policies as burdensome. Using auditing as an example, three of the airports reported changing audit strategies to keep tenants vigilant. They also reported using the data to develop long- or short-term mitigation measures. None found the processes burdensome on airport staff resources. Two of the airports also completed an audit, but reported their security culture as the driver of their successes. Those airports indicated that information gathered through community engagement served as their barometer for additional action, not the audit.

As shown in Table 10-2, the airports with unaccountability between two and three percent also used a variety of strategies to control accountability. These include four Category X airports, one Category I airport, and one Category II airport. All but one reported consistent unaccountability percentages.

The airport whose unaccountability percentage varied more than one percent reported having minimal enforcement, and did not directly communicate ID media rules or responsibilities publicly. Instead, the airport relied solely on the authorized signatory to manage their badged population. Even with the focus on authorized signatory responsibility, that airport operator did not provide any additional communication or training to assist authorized signatories. The airport did report having a strong security awareness program, and had strong practices within its badging office to ensure the staff remained vigilant. This airport may consider enhancing efforts in another area to supplement its strong security awareness and badging office practices. Those requirements may also be imposed by additional regulatory action regarding authorized signatories.

In both tables below, boxes of the same shade in each row represent the airports adopting similar practices, processes, or strategies for comparison purposes.

Table 10-1. Airports with Unaccountability Below Two Percent

	Airport 1	Airport 2	Airport 3	Airport 4	Airport 5	Airport 6
Variability	Varies less than 1%	Varies less than 1%	Varies more than 1%	Varies less than 1%	Varies less than 1%	Varies less than 1%
Enforcement	Active, higher value monetary and non-monetary penalties	Minimal enforcement	Active, higher value monetary and non-monetary penalties	Active, higher value penalty	Active, higher penalty	Active enforcement, lower value penalty
Communication	Authorized signatory responsible, minimal engagement by airport	Some information publicly available and occasional mention at a stakeholder meeting	Authorized signatory responsible, airport actively engages authorized signatory	Information readily available for all interested parties	Information readily available for all interested parties	Authorized signatory responsible, airport actively engages authorized signatory
Auditing	May change strategy or approach to keep tenants vigilant, and attempt to learn from findings	May change strategy or approach to keep tenants vigilant, and attempt to learn from findings	Tailor audit to objective, learn from findings, and work with companies based on results	May change strategy or approach to keep tenants vigilant, and attempt to learn from findings	Standard process	Standard process
Security Awareness	Discuss accountability occasionally if needed	Less proactive	Security culture drives performance	Security culture drives performance	Security culture drives performance	Security culture drives performance
Badging Office	On job training, unwritten policy and procedures	Trained, formal policy and procedures, debriefed, checks and balances	Trained, formal policy and procedures, debriefed, checks and balances	On job training, unwritten policy and procedures	On job training, unwritten policy and procedures	On job training, unwritten policy and procedures
Authorized Signatories	Frequently engage with airport, trained, held accountable	Frequently engage with airport, trained, held accountable	Frequently engage with airport, may engage more if observe poor management practices	Frequently engage with airport, may engage more if observe poor management practices	Frequently engage with airport, may engage more if observe poor management practices	Engage with airport, but no proactive action if authorized signatory struggles
Company	Inadvertently held accountable, TSA engages	Frequent communication but no enforcement	Held accountable with minimal communication	Engaged with, held accountable; trained	Engaged with, held accountable; trained	Held accountable with minimal communication
Renewal	Two years	Mixed access based	Mixed company penalty based	One year	One year	Two years

Table 10-2. Airports with Unaccountability Between Two and Three Percent

	Airport 1	Airport 2	Airport 3	Airport 4	Airport 5	Airport 6
Variability	Varies less than 1%	Varies less than 1%	Varies less than 1%	Varies more than 1%	Varies less than 1%	Varies less than 1%
Penalty	Active, higher value monetary and non-monetary penalties	Active, lower value penalty	Active, higher value monetary and non-monetary penalties	Minimal enforcement	Active, Graduated fee structure	Active, higher value monetary and non-monetary penalties
Communication	Information readily available for all interested parties	Some information publicly available and occasional mention at a stakeholder meeting	Some information publicly available and occasional mention at a stakeholder meeting	Information on application, in training, or on back of badge, i.e., less proactive	Some information publicly available and occasional mention at a stakeholder meeting	Some information publicly available and occasional mention at a stakeholder meeting
Auditing	Standard process	Standard process	Tailor audit to objective, learn from findings, and work with companies based on results	Tailor audit to objective, learn from findings, and work with companies based on results	Standard process	Tailor audit to objective, learn from findings, and work with companies based on results
Security Awareness	Less proactive	Security culture drive performance	Less proactive	Security culture drive performance	Less proactive	Less proactive
Badging Office	Trained, formal policy and procedures, debriefed, checks and balances	On job training, unwritten policy and procedures	Trained, formal policy and procedures, debriefed, checks and balances	Trained, formal policy and procedures, debriefed, checks and balances	Trained, formal policy and procedures, debriefed, checks and balances	On job training, unwritten policy and procedures
Authorized Signatories	Frequently engage with airport, trained, held accountable	Frequently engage with airport, trained, held accountable	Frequently engage with airport, may engage more if observe poor management practices	Engage with airport, but no proactive action if authorized signatory struggles	Engage with airport, but no proactive action if authorized signatory struggles	Less engagement with airport
Company	Engaged with, held accountable	Engaged with, held accountable; trained	Engaged with, held accountable	Not held accountable	Frequent communication but lower value penalty	Held accountable with minimal communication
Renewal	One year	Mixed company penalty based	Two years	Two years	One year	One year

SECTION 11: PHYSICAL ACCESS CONTROL SYSTEMS AND IDENTITY MANAGEMENT SYSTEMS

Developments in PACS and automated IDMS can assist airport operators in controlling ID media accountability. PACS consist of a coordinated network of ID media, electronic readers, field control panels, specialized databases, software, and computers designed to monitor and control traffic through access points. PACS can work independently of, or in tandem with, an IDMS. PACS include the physical assets and infrastructure associated with access control including the credential, readers, locks, databases and associated hardware platforms, scanners, and network infrastructure. In contrast, IDMS are software systems that collect and provide identity information to PACS, and collect and utilize data received from PACS operations. IDMS automate and manage the credentialing process, and can assist with control measures at the beginning of the credentialing process, and later through auditing and terminating access.

The secure portals of an IDMS can provide messages to badge applicants, badge holders, and their respective authorized signatories regarding their responsibilities. In addition to functioning as a portal to receive the data necessary for processing the application, the system can communicate the importance of properly securing and accounting for the credential.

After issuance of the badge, IDMS portals continue to provide signatories with information regarding both their aggregate badged populations and individual badge holders. This information can assist the authorized signatory in better managing accountability. For example, the IDMS will tell authorized signatories when a specific badge holder is approaching renewal, and provides a global status picture of all their badge holders. Additionally, authorized signatories receive email reminders regarding renewal, training requirements, and badge status.

While signatory access through IDMS portals is limited to those applicants sponsored by the signatory, IDMS gives information on the status of ID media across the entire enterprise. The IDMS provides real-time and historical data for trusted agents to analyze. The dashboards for trusted agents provide a status update of accountability for authorized signatories and companies. This information can help formulate policies designed to improve accountability practices of individual companies. For example, a trusted agent can study and monitor a company's turnover rates. Company profile information can assist in tailoring plans for auditing and training to help manage badge accountability.

IDMS can also provide powerful support for the auditing process. The airport can program auditing requirements and the system will automatically generate and email audit information to authorized signatories.

Working in conjunction with PACS, IDMS can help monitor ID media usage. Some PACS can capture and report usage data on their own. However, the IDMS facilitates the collection and dissemination of this data.

The integration of IDMS with PACS can help airports leverage their PACS audit tool to improve accountability. For example, IDMS in conjunction with PACS can prepare and forward reports of badges that are unused for a specified period. The airport can then require the signatory to collect the badge or explain its non-use.

IDMS in conjunction with PACS may also establish accountability, particularly when used with reliable two-factor authentication. Biometric-based systems where PACS can demonstrate that the badge was in possession of the badge holder can provide an affirmative audit in real time.

SECTION 12: RISK MITIGATION FRAMEWORK

Controlling ID media to maintain a high level of accountability presents challenges for airport operators. These challenges are common in the airport community when looking at airports with similar regulatory structures, cultures, or regional economies. Some mitigation measures employed today assist in the short term to prevent unaccountability percentages from reaching reissuance requirements, but these strategies are not long-term solutions an airport can rely on for consistent accountability. Thinking about the concepts of risk-based security, SeMS, and risk mitigation will lead to the development of an ID media-centric risk mitigation framework.

Risk analysis concepts and strategies can help airport operators adopt and manage ID media control programs that fit their specific needs, and position them to best control accountability. Many airports implement risk-based security measures that maximize mitigation with limited resources. Facing a persistent and ever-changing threat environment, airport operators must continuously reassess their ASP and alter strategies to mitigate numerous vulnerabilities within their operating environment. Additionally, airports must tailor their security programs and strategies to the overarching airport culture.

Airports currently use their security culture to manage risks. As presented in *PARAS 0009 Guidance for Security Management Systems (SeMS)*, an SeMS helps establish and maintain security cultures. When adopting SeMS principles, airports integrate risk mitigation strategies with their broader airport business and risk strategies to create a framework for managing their security program. SeMS scalability allows airports to tailor their security needs based on their resources. An SeMS reduces an airport's exposure to security risks by identifying vulnerabilities and subsequently managing them. ID media accountability and control programs must exist within the airport's security program and broader airport culture to achieve risk-based security goals and mitigate vulnerabilities.

Like SeMS, the DHS Policy for Integrated Risk Management (IRM) recognizes that successful risk management is a collaborative activity requiring implementation across the entire security enterprise. This helps ensure that department components use consistent risk management strategies and that there is a shared perspective of the security challenges. The risk management program is able to be scaled and tailored to meet specific needs and security cultures. Appendix F includes an IRM summary. DHS risk management programs support open and direct communication as security decisions involve a wide array of stakeholders. Both SeMS and IRM seek to apply a systems approach to decision-making.

Risk mitigation concepts can assist airports in fine-tuning their ID media accountability and control strategies within their broader airport culture. Numerous models of risk management exist, and no one model perfectly addresses the issue of badge accountability. However, the principles that underlie these models may help airport operators better understand and manage the risks inherent in managing badge issuance.

The risk mitigation process begins by identifying the risks requiring mitigation. An understanding of risk is the result of a risk assessment process. Risk assessments review the entire enterprise to determine risk factors implicated by failures of ID media accountability.

Risk mitigation theories like Enterprise Security Risk Management (ESRM) provide insights into identifying risk. ESRM proposes the identification and evaluation of risk in the larger context of enterprise-wide goals and objectives. Common risks related to failure to control ID media include:

- Financial risk of reissuing badges in the event unaccountability exceeds five percent
- Human resource risks to the airport and shareholders in conjunction with reissuance
- Legal risks associated with failure to meet federal accountability standards
- Political risks in the event unaccountability levels require reporting to Congress
- Brand or reputation risks concerning the ability of the airport to competently monitor a critical security program

These suggested risks do not represent an exhaustive list, but should serve as a starting point for analysis. Understanding these risks can help ID media managers explain the importance of imposing and enforcing accountability measures. SeMS can help by communicating the values and objectives of the airport to the rest of the staff. This creates a safer environment where everyone participates in the security culture.

A clear risk picture assists in communicating the need for support and resources to executive-level personnel. It can also assist in explaining to trusted agents, authorized signatories, and the badged population the reasons for and importance of accountability measures.

In addition to establishing and executing an assessment of risk, the development of a risk mitigation strategy requires identification and assessment of measures to mitigate risk. Some of those measures involve examining internal changes within the airport's control. Other measures address external factors contributing to risk.

Identifying and evaluating risk mitigation methods is an important part of the evaluation process. Developing a listing of risk mitigation measures presents a good starting point for an overall evaluation. Common measures across the industry include but are not limited to:

- Fines and penalties for noncompliance
- Incentives for compliance level
- Communication with stakeholders
- Security awareness through the security culture, training, and program
- Authorized signatory engagement, training, and accountability
- Trusted agent engagement, training, and accountability
- Auditing practices, robustness of the process, and feedback loop to enforcement
- Adjusting expiration periods for the entire badged population, specific access levels, or for specific companies

Internal measures purely within the control of the airport are easier to fashion. Examples include setting expiration periods or developing audit schedules and focuses. Measures seeking to govern the conduct of external actors are more difficult. Examples include training and communication strategies for authorized signatories and companies.

When designing risk mitigation measures, inclusion of stakeholder input is valuable. Establishing a formal or informal group to evaluate risk mitigation measures, and developing communication strategies to encourage buy-in, can assist in developing an effective risk mitigation strategy.

With risks clearly defined, mitigation measures identified, and stakeholder inputs considered, the airport can assess what measures can be implemented with available resources. The airport must look at this issue holistically and consider the overall risk that unaccountability presents to their facility along with other threats that it must mitigate. Based on that assessment, an airport can finalize the ID media control policies and have a baseline of performance to measure against. Appendix E (Risk Mitigation Worksheet) offers a sample risk mitigation framework worksheet for ID media accountability and control.

SECTION 13: CONCLUSION

Accountability of ID media presents a challenge for airport operators because of the dynamics of the airport community and continued focus on unaccountability from external stakeholders. It has received attention since airport access restrictions were introduced in 1990, and will likely continue to be scrutinized as insider threat or other security events occur.

The data collected for this report shows that an ID media program with balanced and complementary measures will succeed, and that successful strategies are not identical. Airport operators must evaluate the demands and challenges of their operating environment to develop successful policies. Many airports face high turnover in their badged populations, and have tenants that fail to prioritize accountability or view penalties as the cost of doing business. These airports also face internal challenges, including resource constraints, local laws and administrative processes, and overarching priorities that may conflict with control policies. These external and internal factors mandate a balanced and complementary approach to controlling ID media. Airport operators should consider the following:

- Does the ID media program mesh with the airport's overarching strategic plan and direction?
- Do the control processes, practices, and strategies have airport leadership and political support?
- How should the airport prioritize resources to control ID media?
- How does the airport community respond to responsibilities, enforcement actions, and outreach campaigns?
- Do the control processes, practices, and strategies achieve consistently low unaccountability percentages year to year?

REFERENCES

- Armstrong, Michael. *Armstrong's Book of Human Resource Management Practice*. London: Kogan Page, 2014.
- "Auditing Human Subjects Research." *Indiana University*. Accessed June 10, 2019. https://www.tradoc.army.mil/Portals/14/Documents/RAS_Strategy.pdf.
- "Aviation Security." Code of Federal Regulation, Title 14 (1997) FAA Rule 107 (62 FR 41760). August 1997. <https://www.gpo.gov/fdsys/pkg/FR-1997-08-01/pdf/97-19698.pdf>.
- "Aviation Security." Code of Federal Registration, Title 14 (1997) FAA Rule 107 (66 FR 37274). July 2001. <https://www.gpo.gov/fdsys/pkg/FR-2001-07-17/pdf/01-16994.pdf>.
- Aviation Security Advisory Committee. "Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control." Aviation Security Advisory Committee, April 8, 2015. <https://www.tsa.gov/sites/default/files/asac-employee-screening-working-group-04-15.pdf>.
- Aviation Security Advisory Committee. "Report of the Aviation Security Advisory Committee on Insider Threat at Airports." Aviation Security Advisory Committee, July 19, 2018. https://www.tsa.gov/sites/default/files/asacinsidethreatreport_072018.pdf.
- Aviation Transportation Security Act of 2001 (ATSA). Public Law 107-7. <https://www.gpo.gov/fdsys/pkg/PLAW-107publ71/pdf/PLAW-107publ71.pdf>.
- Barich. "Enhancing Communication & Collaboration Among Airport Stakeholders," National Safe Skies Alliance PARAS 0003 (January 2017).
- Beer, Michael, and Russell A. Eisenstat. "Developing an Organization Capable of Implementing Strategy and Learning." *Human Relations* 49 (1996): 597-619.
- Blank, Joshua D. "Collateral Compliance." *University of Pennsylvania Law Review* 162, no. 4 (March 2014): 719-800. <http://dx.doi.org/10.2139/ssrn.2032788>.
- "Compliance Audits." *American Institute of Certified Public Accountants*, AU Section 801 (n.d.): 2463-2486. <https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00801.pdf>.
- "Concepts and Theories of Auditing." *UK Essays*. Last modified November 2018. <https://www.ukessays.com/dissertation/examples/accounting/theory-of-auditing.php>.
- "Contingency Theory." *Value Based Management*. Accessed June 10, 2019. https://www.valuebasedmanagement.net/methods_contingency_theory.html.
- Davoren, Julie. "Contingency Theory in Auditing." *Houston Chronicle*. Accessed June 10, 2019. <http://smallbusiness.chron.com/contingency-theory-auditing-46110.html>.

- Department of Homeland Security. “Access Control Systems.” *Code of Federal Regulations*, Title 49 (2010): 333-334. <https://www.gpo.gov/fdsys/pkg/CFR-2010-title49-vol9/pdf/CFR-2010-title49-vol9-sec1542-207.pdf>.
- Department of Homeland Security. “Identification Systems.” *Code of Federal Regulations*, Title 49 (2010): 338-339. <https://www.gpo.gov/fdsys/pkg/CFR-2010-title49-vol9/pdf/CFR-2010-title49-vol9-sec1542-211.pdf>.
- Department of Homeland Security. “Risk Management Fundamentals,” Homeland Security Risk Management Doctrine, (April 2011).
- Department of Homeland Security. “Security of the Secured Area.” *Code of Federal Regulations*, Title 49 (2010): 332. <https://www.gpo.gov/fdsys/pkg/CFR-2010-title49-vol9/pdf/CFR-2010-title49-vol9-sec1542-201.pdf>.
- Department of Homeland Security. “Security of the Air Operations Area (AOA).” *Code of Federal Regulations*, Title 49 (2010): 327-328. <https://www.gpo.gov/fdsys/pkg/CFR-2013-title49-vol9/pdf/CFR-2013-title49-vol9-sec1542-203.pdf>.
- Department of Homeland Security. “Security of the Security Identification Display Area (SIDA).” *Code of Federal Regulations*, Title 49 (2010): 333. <https://www.gpo.gov/fdsys/pkg/CFR-2010-title49-vol9/pdf/CFR-2010-title49-vol9-sec1542-205.pdf>.
- Department of Homeland Security. “Training.” *Code of Federal Regulations*, Title 49 (2010): 339-340. <https://www.gpo.gov/fdsys/pkg/CFR-2010-title49-vol9/pdf/CFR-2010-title49-vol9-sec1542-213.pdf>.
- 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).
- Department of Homeland Security Office of Inspector General. “TSA’s Oversight of the Airport Badging Process Needs Improvement,” OIG-11-95 (July 2011).
- Department of Transportation Office of Inspector General. “Controls Over Airport Identification Media.” Federal Aviation Administration. Report No.: AV-2001-010. December 7, 2000.
- Elman, Jeremy. “Are Financial Penalties Effective?” Last modified September 12, 2008. <https://www.rsm.global/australia/insights/technology-risks/are-financial-penalties-effective>.
- “Employment Standards.” *Code of Federal Registration*, Title 14 (1991) FAA Rule 107 (56 FR 41412). August 1991. <https://cdn.loc.gov/service/ll/fedreg/fr056/fr056161.pdf>.
- Executive Order 12686 – Report of the President’s Commission on Aviation Security and Terrorism. May 1990. <https://ia800402.us.archive.org/28/items/PCASTreport/PCASTreport.pdf>.
- FAA Extension Safety and Security Act of 2016. Public Law 114-190, Section 3404.

<https://www.congress.gov/bill/114th-congress/house-bill/636/text>.

FAA Reauthorization Act of 1996. Public Law 104-264.

<https://www.congress.gov/104plaws/publ264/PLAW-104publ264.pdf>.

Federal Aviation Administration Office of Inspector General. "Controls over Airport Identification Media," AV-2001-010 (December 2000).

Gluck, Kevin A., et al. "Prospective Comments on Performance Prediction for Aviation Psychology," in *Advances in Aviation Psychology: Improving Aviation Performance through Applying Engineering Psychology*, eds. Michael A. Vidulich and Pamela S. Tsang. Boca Raton, FL: CRC Press, 2019.

Gneezy, Uri, and Aldo Rustichini. "A Fine is a Price." *The Journal of Legal Studies* 29, no. 1 (January 2000): 1-17. DOI: 10.1086/468061.

Gore, Al. "White House Commission on Aviation Safety and Security: Final Report to President Clinton." February 12, 1997. <https://fas.org/irp/thret/212fin~1.html>.

Hedge, Jerry W., et al. *Implementing Organizational Interventions: Steps, Processes, and Best Practices*. San Francisco: Jossey-Bass, 2002.

Ittonen, Kim. "A Theoretical Examination of the Role of Auditing and the Relevance of Audit Reports." *Vaasan Yliopiston Julkaisuja* 61 (2010): 1-64.

Jastrzembski, Tiffany S., et al. "Personalizing Training to Acquire and Sustain Competence Through Use of a Cognitive Model." *Augmented Cognition. Enhancing Cognition and Behavior in Complex Human Environments: AC 2017* 10285 (2017): 148-161.

Jastrzembski, Tiffany S., et al. "The Predictive Performance Optimizer: An Adaptive Analysis Cognitive Tool for Performance Prediction." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 53, no. 21 (October 2009): 1642-46. doi:10.1177/154193120905302102.

King, N. "Innovation at Work: The Research Literature," in *Innovation and Creativity at Work: Psychological and Organizational Strategies*, eds. Michael A. West and James L. Farr. New York: Wiley, 1990, 15-59.

Lopez, David, and Oscar Pastor. "Comprehensive Approach to Security Risk Management in Critical Infrastructure and Supply Chains." *Information & Security: An International Journal*, vol 29, 2013, 69-76.

McLeod, Saul. "Skinner-Operant Conditioning." *Simply Psychology*. Last modified 2018. <https://www.simplypsychology.org/operant-conditioning.html>.

Nagin, Daniel S. "Deterrence in the 21st Century." *Crime and Justice* 42, no. 1 (August 2013): 199-263. doi:10.1086/670398.

National Association of School Psychologists. "Effective (and Easy) Communications: Tips for School Psychologists." *National Association of School Psychologists*. Accessed May 21, 2019.

https://www.nasponline.org/Documents/Research%20and%20Policy/Advocacy%20Resources/Exhibit_H4.pdf.

Olson, David L., and Desheng Wu. "Enterprise Risk Management Models." Springer, 2010.

Petruzzi, John, and Rachelle Loyear. "Improving organizational resilience through enterprise security risk management." *Journal of Business Continuity & Emergency Planning*, volume 10 number 1, 2016.

Rees, C., et al. "Employee Voice and Engagement: Connections and Consequences." *International Journal of Human Resource Management* 24, no.14 (2013): 2780-2798.

Rieder, R., et al. "Guidance for Security Management Systems (SeMS)," National Safe Skies Alliance PARAS 0009 (March 2018).

RTCA, "Standards for Airport Access Control Systems," *DO-230UI* (June 2018).

Schram, Pamela J., and Stephen G. Tibbetts. *Introduction to Criminology: Why Do They Do It?* Thousand Oaks, CA: SAGE Publications, 2018.

The Aviation Security Improvement Act of 1990. Public Law 101-604.
<https://www.gop.gov/fdsys/pkg/STATUTE-104/pdf/STATUTE-104-Pg3066.pdf>.

"The Social Cognitive Theory." *Boston University School of Public Health*. Last modified August 29, 2018. <http://sphweb.bumc.bu.edu/otlt/MPH/Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories5.html>.

Tomlinson, Kelli D. "An Examination of Deterrence Theory: Where Do We Stand?" *Federal Probation Journal* 80, no. 3 (December 2016): 33-38.
https://www.uscourts.gov/sites/default/files/80_3_4_0.pdf.

Transportation Research Board, Airport Cooperative Research Program. "A Guidebook for Safety Risk Management for Airports." ACRP 131. 2015.

U.S. Government Accountability Office, "TSA Has Made Progress Implementing Requirements in the Aviation Security Act of 2016," GAO-17-662 Aviation Security (September 2017).
<https://www.gao.gov/assets/690/686992.pdf>.

Visentin, Lisa. "City of Sydney Shelves Library Fines for Four Years After 70,000 Overdue Items Returned." *The Sydney Morning Herald*. Last modified July 7, 2017.
<https://www.smh.com.au/national/nsw/city-of-sydney-shelves-library-fines-for-four-years-after-70000-overdue-items-returned-20170707-gx6lcl.html>.

Walsh, Matthew M., et al. "Evaluating the Theoretic Adequacy and Applied Potential of Computational Models of the Spacing Effect." *Cognitive Science* 42 (June 2018): 644-691.
<https://doi.org/10.1111/cogs.12602>.

Yue, Carol. "Need to remember something? Try forgetting it!" *Psychology in Action*. Last modified September 21, 2011. <https://www.psychologyinaction.org/psychology-in-action-1/2011/09/21/need-to-remember-something-try-forgetting-it>.

APPENDIX A: POLICY ALTERNATIVE CHEAT SHEET

ID Media Issuance

- Include basic authorized signatory and badge holder responsibility language in the application.
- Require the applicant to sign a responsibility sheet before issuing the badge.
- Issue only one badge to individuals who work for multiple employers.
- Set renewal periods based on operational concerns other than accountability.
- Reduce renewal periods to less than a year.
- Implement a graduated renewal period.
- Require seasonal employee and temporary contractor badges to expire on their last day of work.

Training

- Cover basic responsibilities in new badge holder training.
- Require all badge holders to participate in recurrent training that includes reinforcement of badge accountability responsibilities, penalties, and security awareness.
- Facilitate biannual voluntary peer-to-peer authorized signatory training and strategy meetings.
- Offer quarterly in-person training for authorized signatories.
- Offer drop-in office hours for authorized signatories to meet with the airport trusted agents to discuss accountability management practices.
- Require authorized signatories to discuss responsibilities with their badge holders monthly or quarterly.

Communication

- Make rules, penalties, and policies readily available for companies, authorized signatories, and badge holders.
- Engage stakeholders through outreach campaigns to strengthen the airport's security culture.
- Provide authorized signatories access to a reference guide.
- Provide authorized signatories with a responsibility summary sheet reminding them of their accountability responsibilities and where to receive assistance.

Enforcement

- Implement a penalty structure that includes a combination of fines and non-monetary penalties directed at companies, authorized signatories, and badge holders.
- Implement a non-monetary penalty system for companies with consistently high unreturned badge percentages.
- Penalize companies when their unaccountability rates exceed a percentage threshold.
- Implement a graduated penalty structure that increases based on the level of noncompliance.
- Refund monetary penalties if a company or individual can mitigate unaccountability within a specific period.
- File a police report for unreturned badges.
- Include unreturned badge fees in construction contracts.
- Include unreturned badge fees in the FBO or individual hangar lease agreements.
- Host a Badge Return Moratorium to mitigate a rising unaccountability rate.

Badging Office and Trusted Agents

- Pursue unreturned or lost media with the same vigor whether it is expired or unexpired.
- Document policies and procedures for trusted agents and badging office staff.
- Create detailed instruction sheets for badging office employees to reference.
- Engage badging office employees to show them why their role is important and how it affects airport security.
- Audit airport control practices.
- Require tenants to review and attest to continued need for secured area access.
- Deactivate badges that remain unused after a specified amount of time.

Auditing

- Implement an audit strategy that leads the airport's decision-making for ID media control efforts.
- Implement an auditing strategy that meets the regulatory baseline
- Conduct additional audits for companies that have trouble managing their badged population.
- Verify that badge holders possess their credentials by checking access control swipe records.

APPENDIX B: BADGE HOLDER BROCHURE

ID MEDIA BADGES

Accountability and control of
airport-issued ID media is a
critical component of overall
airport security.
TSA oversees federal
regulations that require
airport operators to establish
an identification system that
includes the issuance of ID
media badges.



Insert a photo from your airport

Your Organization
Primary Business Address
Your Address Line 2
Your Address Line 3
Your Address Line 4
Phone: 555-555-5555
Fax: 555-555-5555
E-mail: someone@example.com

How To Be A Responsible Badgeholder

Your Organization
Your business tag line here.

YOUR LOGO
HERE

Basic Information



ID Badges must...

- have a valid photo, badge number, expiration date, employee name and company name.
 - be displayed at all times above the waist on the outermost garment of clothes.
 - Not be used by others. There is only one badge per person.
 - not be expired. Expired badges must be immediately returned to the badging office.
- Badgeholders must...
- securely close doors, vehicle gates, and bag belts after being accessed.
 - ensure no one is entering secure areas behind them.
 - not bypass TSA screening checkpoints while traveling.

Failure to comply with these guidelines endangers airport security and may result in penalties or badge revocation.

The Badging Office

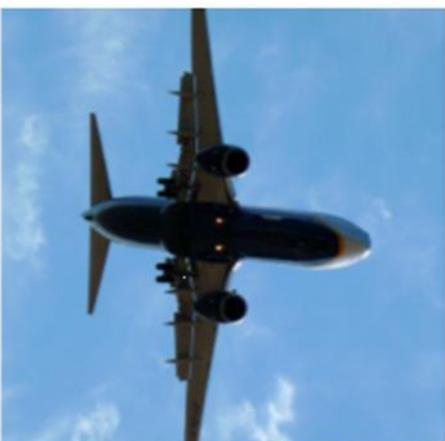
- Badges are airport property and must be returned to the airport badging office upon termination, resignation, leave of absence, medical leave, retirement, or any other time airport access is no longer required.
- Badges should never be thrown away, destroyed, shredded, or discarded in anyway. They must always be returned to the badging office.
- Expired badges must be returned to the badging office.
- Lost or stolen badges must be reported to the badging office so that the badges may be deactivated. If the badge is found, do not use it until otherwise directed.
- Badge replacement fees are \$xx for the first badge. Subsequent replacements are \$xx.
- Badging Office number: xxx-xxx-xxxx

Escorting

- Visitors with an operational need to be in a restricted area may only be escorted by those with ID badges that say "ESCORT"
- You must maintain positive control over the visitor(s) you are escorting at all times.
- Badgeholders without their badge (lost, left at home, ect.) may not be escorted into restricted areas by another badgeholder.
- You may not escort someone with a revoked, suspended, or expired badge.
- You may not escort someone who was disqualified from acquiring a security badge.
- Escort authority can only be transferred to another authorized badgeholder.

Accountability

- If you see someone in a restricted area who is not displaying their badge, request to see their badge.
- If they show it to you, check that they match their picture and that it has not expired.
- If they do not have a valid badge, call _____ at xxx-xxx-xxxx.
- If you feel too unsafe to talk to them, call _____ and provide a detailed description of the person and the location.
- All badgeholders must cooperate by showing their badges if requested.
- TSA conducts regular badge tests.



Insert a photo from your airport

APPENDIX C: BADGE HOLDER FACT SHEET

XXX Airport Authority ID Media Accountability Badge Holder Responsibilities

- Maintain control of your badge and leave it in a secure place when you are not at work.
- Report a lost or stolen badge immediately to your authorized signatory or the Badging Office.
 - Badging Office Phone: XXX-XXX-XXXX
 - If after hours, please contact Airport Operations: XXX-XXX-XXXX
- File a police report if your badge is stolen.
 - The airport will require proper documentation to avoid lost badge penalties.
- Return your badge immediately to your authorized signatory, the Badging Office, or place it in the mail (no postage required) when unescorted access to the secured area is no longer needed.
 - Badging Office Address:
 - If after hours, please return your badge to airport operations: Address

Failure to comply with these guidelines endangers airport security and may result in penalties or badge revocation.

APPENDIX D: ASAC ID MEDIA AUDIT RECOMMENDATIONS

Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control

Appendix 2, Auditing and Internal Controls Best Practices

1. Proof-of-Employment Audit
Require proof of active employment for each badge holder which may include, but is not limited to, a company time and attendance record, human resources (HR) or payroll record, or letter from HR or company headquarters confirming employment. This audit is one of the most effective internal controls to identify badge discrepancies resulting from a failure of the authorized signatory to notify the airport to deactivate the badge of a separated employee.
2. Change-in-Employment-Status Policy
Implement a policy to address change in employment status. The policy should govern the custody and status of security badges of individuals whose employment status has changed in accordance with the following conditions: Family and Medical Leave Act (FMLA), worker's compensation, military service, reassignment, or other extended personal time off, etc., which no longer supports the operational need to maintain possession of a badge. Authorized signatories are required to temporarily deactivate and maintain secure custody and control of the media. Long-term absences will require the media to be permanently deactivated. This policy reduces the number of lost and unaccountable badges during extended absences from work.
3. Field Badge Audit
Conduct a random field badge audit at the authorized signatory's place of business. During the site inspection, the auditor conducts a document review and interview of the authorized signatory to assess compliance with badging requirements and information protection (i.e., Sensitive Security Information and personally identifiable information), and best practices.
4. Work Schedule Audit
Reconcile the badge holder's work schedule with Access Control System (ACS) transactions during a specified period to identify access anomalies or irregularities, such as an employee using his/her badge at the airport outside of work hours. This audit may be conducted using manual or automated reconciliation of ACS and work schedule records. The company's authorized signatory provides the work schedule of randomly selected employees to airport security representatives for comparison with the employee's badge activity utilizing ACS records. Insider threat software procured by an airport operator offers this automated capability; however, a data feed from the employer, e.g., aircraft operator is required.
5. Deactivated Badge Use Audit
Conduct a deactivated badge audit to identify unauthorized use of a deactivated badge (e.g., access was attempted but not granted) by performing a forensic review of ACS transactions.
6. Reverse Badge Audit
Conduct a reverse badge audit which requires the company's authorized signatory to provide an internal report of their badge holders that is reconciled with the control record of the security badge office to identify discrepancies.

7. Badge Deactivation for Non-Use

Consider deactivation of badges which have been inactive for a defined period. This measure will assist in reducing the lapse time of badges not immediately reported as missing or that are no longer needed. If an employee's badge is deactivated as a result of inactivity, the company is required to provide the security badge office with a legitimate reason for the inactivity (e.g., FMLA, military leave, etc.) upon which the badge may be reactivated. During extended absences, the employee may need to submit a new badge application. Exemptions based on specific employee assignments and positions will be necessary.

8. Biometric Confirmation of Identity for Badge Issuance and Random Auditing

Capture a biometric template of SIDA applicants (e.g., fingerprints or other biometric) at the time of submitting fingerprints for CHRC processing. Confirm the identity of applicant at the time of badging by matching the individual's biometrics to the template originally captured. Retain the biometric template of each individual on their SIDA card for random checks with mobile biometric readers in the secured area to confirm the identity of the card holder and ensure that a card is not being used by someone other than the person authorized for SIDA privileges.

APPENDIX E: RISK MITIGATION WORKSHEET

I. Define Airport Goals and Objects

- a. Airport Mission and Objectives
- b. Airport Security Mission and Priorities
- c. Risk Management Process
- d. Unaccountability Goal
- e. Stakeholder Considerations
- f. Risk Tolerance

II. Identify Risks Requiring Mitigation

- a. Security Culture
 - i. Everyone at the airport is involved*
 - ii. Values of the staff are aligned with the airport mission*
- b. Vulnerabilities
 - i. Internal*
 - ii. External*
- c. Likelihood of the Event Occurring
- d. Consequences if the Event Occurs

III. Mitigation Measures

- a. Internal
 - i. Setting expiration periods*
 - ii. Developing audit schedules and focuses*
- b. External
 - i. Authorized signatory and company training*

IV. Stakeholder Inputs

- a. Threat and risk briefings are a standing item on the Board meeting agenda**
- b. Effective two-way communication**

V. Policy Decisions

- a. Develop Alternatives**
 - i. Review lessons learned*
- b. Risk Management Strategy**
 - i. Risk Acceptance*
 - ii. Risk Avoidance*
 - iii. Risk Control*
 - iv. Risk Transfer*
- c. Document the Decision**
- d. Assess Success**
- e. Guard Against Unintended Adverse Consequences**

APPENDIX F: DHS INTEGRATED RISK MANAGEMENT

DHS's risk management process, as defined in its IRM policy, evaluates internal and external sources of risk and is composed of six steps:

- **Defining and framing the context of decisions and related goals and objectives.** This can involve setting up a risk analysis team for complex problems. Team members must factor in political and policy concerns, mission needs, stakeholder interests, and risk tolerance levels. This step will shape the rest of the process.
- **Identifying the risks associated with goals and objectives.** This approach will yield a broad list of potentially adverse outcomes that will assist in the identification of mitigation efforts and resources. Team members should define elements affected by the risk, and think about the risks in terms of “risk to” and “risk from.”
- **Analyzing and assessing the identified risks.** Team members should determine a methodology, gather data, execute the methodology, validate the data, and analyze the outputs.
- **Developing alternative actions for managing the risks, creating opportunities, and analyzing the costs and benefits of those alternatives.** This can be done by reviewing lessons learned from previous incidents and developing cost estimates for risk management actions.
- **Deciding among alternatives and implementing that decision.** Team members need to consider the feasibility of implementing options, and how various alternatives affect and reduce risk.
- **Monitoring the implemented decision and comparing observed and expected effects to help influence subsequent risk management alternatives and decisions.** This includes evaluating and monitoring performance to determine whether the implemented risk management options achieved the stated goals and objectives and guarding against unintended adverse impacts.

These six steps do not always have to occur in the given order. Based on the specific situation, and time and resource constraints, the process may be executed in a less structured manner.