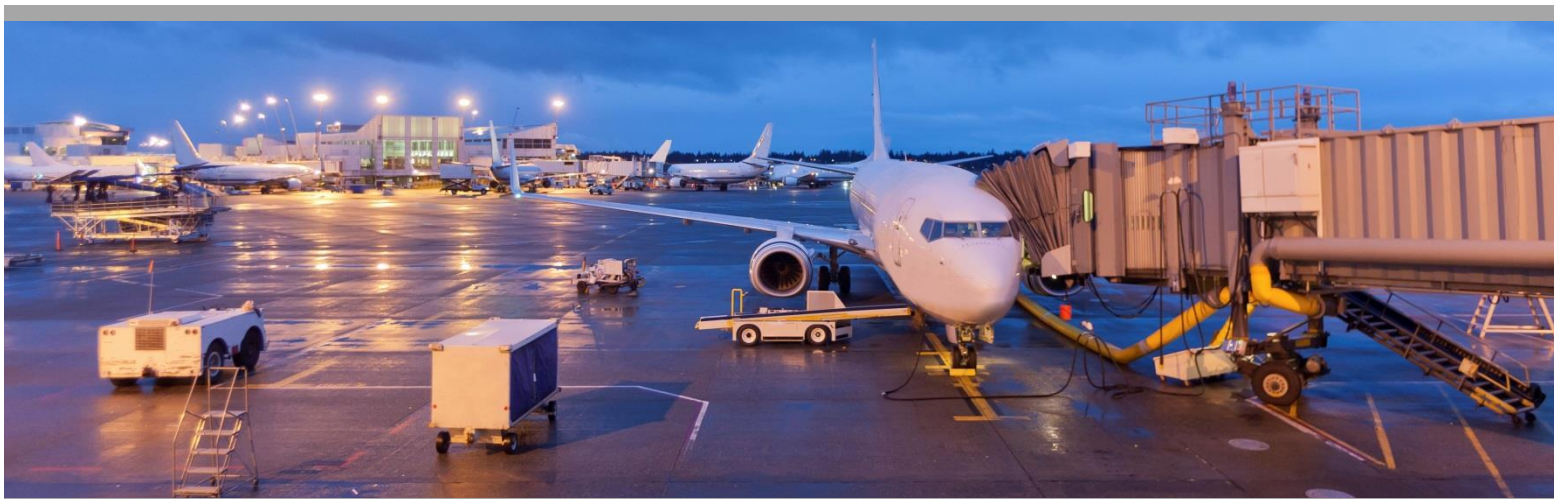




PARAS

PROGRAM FOR APPLIED
RESEARCH IN AIRPORT SECURITY



PARAS 0063

July 2026

Considerations for Full Employee Screening at Airports

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Scott Houston, Principal Investigator

Lee Kair

The Chertoff Group

Kim Dickie

KPD Consulting, LLC

Mike Everson

Airport Law Enforcement Consultant

Michele Freadman

M. Freadman Consulting, LLC

© 2026 National Safe Skies Alliance, Inc. All rights reserved.

COPYRIGHT INFORMATION

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

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

NOTICE

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

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

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

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

NATIONAL SAFE SKIES ALLIANCE, INC.

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

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

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

Through PARAS (Program for 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 PARAS Program Manager*

PARAS 0063 PROJECT PANEL

Andy Entrekin *TransSolutions*

Mark Inzana *Denver International Airport*

Abedoon Jamal *San Francisco International Airport*

Joseph Job *Savannah Airport Commission*

Ryan Leneweaver *Allied Universal*

Terry McHugh *Seattle-Tacoma International Airport*

Sean Michael *Port of Portland*

Doug O'Mara *Global Elite Group*

Mervin Peter *The Port Authority of New York and New Jersey*

Swapnil Shah *Ronald Reagan Washington National Airport*

Jerome Woodard *Dallas Fort Worth International Airport*

AUTHOR ACKNOWLEDGMENTS

The PARAS 0063 Research Team would like to acknowledge the following organizations and individuals for their contributions to the development of this research. First, Safe Skies and Jessica Grizzle for facilitating the research and providing guidance. Second, the PARAS 0063 Project Panel members, who provided significant review and thoughtful comments on the research. And finally, the Research Team extends its gratitude to the aviation professionals from airports, air carriers, and contract security providers who shared their time, expertise, and operational insights throughout this project. Their willingness to participate in interviews and focus groups made this research possible, and their candid perspectives greatly enriched the final product. We are withholding acknowledgment of individuals and their organizations to protect the confidentiality of the interviews.

CONTENTS

SUMMARY	x
PARAS ACRONYMS	xi
ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS	xii
SECTION 1: INTRODUCTION AND CURRENT IMPLEMENTATION LANDSCAPE	1
1.1 Current State of Employee Screening Implementation	2
1.1.1 Implementation Approaches	2
1.1.2 Patterns by Airport Category	2
1.2 Strategic Insights	4
1.3 Emerging Trends	5
SECTION 2: NEEDS ASSESSMENT AND BUSINESS CASE	7
2.1 Understanding the Need and Building the Business Case for Full Employee Screening	7
2.1.1 Needs Assessment	7
2.1.2 Risk Assessment	8
2.1.3 Root Cause Analysis	9
2.1.4 Cost-Benefit Analysis	10
2.1.5 Business Case Development	11
2.2 Key Findings	12
2.2.1 Security Incidents as Implementation Drivers	12
2.2.2 Proactive Implementation Approaches	13
2.2.3 Full Employee Screening Program Costs	13
2.2.4 Infrastructure and Space Challenges	14
2.2.5 Executive Leadership and Organizational Culture	15
2.3 Recommendations and Implementation Guidance	15
SECTION 3: FUNDING CONSIDERATIONS	18
3.1 Understanding Program Costs and Funding Challenges	18
3.1.1 Budget Planning and Cost Analysis	18
3.1.2 Cost Allocation Models	19
3.1.3 Funding Sources	20
3.1.4 Cost Management Strategies	25
3.2 Recommendations and Implementation Guidance	25
SECTION 4: PROGRAM SCOPE	27
4.1 Defining Program Scope and Screening Boundaries	27
4.1.1 Establishing Screening Boundaries	28
4.1.2 Scalability Considerations	29
4.1.3 Phased Implementation Approaches	29
4.1.4 Managing Population Exemptions	30
4.2 Recommendations and Implementation Guidance	30

SECTION 5: STAKEHOLDER ENGAGEMENT	33
5.1 Building Consensus Through Stakeholder Engagement	33
5.1.1 Identifying Stakeholders	33
5.1.2 Strategic Communication Approaches	33
5.1.3 Employee Communication and Education	34
5.1.4 Addressing Stakeholder Concerns	34
5.1.5 Facilitating Collaborative Program Development	35
5.1.6 Developing Continuous Engagement Mechanisms	35
5.2 Recommendations and Implementation Guidance	35
SECTION 6: SCREENING INFRASTRUCTURE	38
6.1 Strategic Infrastructure Planning and Checkpoint Design	38
6.1.1 Leveraging Capital Projects for Screening Infrastructure	38
6.1.2 Airports Without Near-Term Capital Projects	39
6.1.3 Remote Screening Locations	40
6.1.4 Contingency Access Planning	41
6.1.5 Space and Infrastructure Needs	41
6.2 Recommendations and Implementation Guidance	42
SECTION 7: SCREENING TECHNOLOGY	45
7.1 Technology Selection and Investment Decisions	45
7.1.1 Technology Options and Capabilities	45
7.1.2 Technology Investment Decision Criteria	47
7.1.3 Acquisition Strategies	47
7.1.4 Leveraging Cooperative Purchasing Programs	48
7.1.5 Security Equipment Cost Management	49
7.1.6 Technology Life Cycle Management	49
7.1.7 Technology Refresh Planning	50
7.2 Recommendations and Implementation Guidance	50
SECTION 8: PROHIBITED ITEMS AND TOOLS OF THE TRADE	53
8.1 Developing Prohibited Items and Tools-of-Trade Management Policies	53
8.1.1 Prohibited Items List Development	53
8.1.2 Tools-of-Trade Authorization and Accountability Processes	53
8.1.3 Prohibited Items Discovery Procedures	57
8.2 Recommendations and Implementation Guidance	57
SECTION 9: OPERATING PROCEDURES	60
9.1 Establishing Operating Procedures	60
9.1.1 SOP Development Approaches	60
9.1.2 SOP Content and Structure	60
9.1.3 SOP Relation to ASP	61

9.1.4	SOP Maintenance and Updates	61
9.1.5	Alarm Resolution Processes	62
9.1.6	Incident Response Protocols	63
9.1.7	Documentation and Reporting Requirements	64
9.2	Recommendations and Implementation Guidance	64
SECTION 10: WORKFORCE MANAGEMENT		67
10.1	Staffing Model Considerations	67
10.1.1	Direct Airport Employee Model	67
10.1.2	Security Contractor Model	68
10.1.3	Hybrid Model	69
10.1.4	Data-Driven Staffing and Scheduling	70
10.1.5	Staffing Efficiency and Performance	71
10.1.6	Recruitment and Retention Challenges	71
10.2	Recommendations and Implementation Guidance	72
SECTION 11: TRAINING AND QUALITY ASSURANCE		74
11.1	Building Competency and Maintaining Effectiveness	74
11.1.1	Initial Training Programs	74
11.1.2	Recurrent Training Requirements	75
11.1.3	Training Development and Cross-Training Programs	75
11.1.4	Quality Control and Testing Programs	76
11.1.5	Performance Metrics and KPI Development	77
11.1.6	Continuous Improvement Practices	79
11.2	Recommendations and Implementation Guidance	79
SECTION 12: REGULATORY CONSIDERATIONS		84
12.1	Regulatory Framework and ASP Integration	84
12.1.1	ASP Content and Amendment Process	84
12.1.2	TSA Coordination for Alarm Resolution	85
12.1.3	TSA AWS Requirements	86
12.1.4	Compliance with Airport Security Rules and Regulations	86
12.1.5	ICAO Standards and International Agreements	88
12.2	Recommendations and Implementation Guidance	89
SECTION 13: LEGAL CONSIDERATIONS		91
13.1	Understanding Legal Issues and Considerations for Full Employee Screening	91
13.1.1	Legal Authority for Full Employee Screening	91
13.1.2	Liability Management and Risk Mitigation	93
13.1.3	No-Touch Policies and TSA Referral	93
13.1.4	Pat-Down Procedures and Risk Mitigation	94
13.1.5	Insurance and Risk Transfer Considerations	94

13.1.6	Camera Coverage and Documentation	94
13.1.7	Privacy Protections	94
13.1.8	Employee Rights and Workplace Accommodations	95
13.2	Recommendations and Implementation Guidance	95
APPENDIX A: SAMPLE QUALITY ASSURANCE FORMS FOR EMPLOYEE SCREENING OPERATIONS		A-1

TABLES & FIGURES

Table 1.	Employee Screening Implementation Status	3
Table 2.	AIP and PFC Eligibility for Full Employee Screening Program Components	24
Table 3.	Screening Technology Implementation by Airport Category	46
Table 4.	Direct Airport Employee Staffing Model	68
Table 5.	Security Contractor Staffing Model	69
Table 6.	Hybrid Staffing Model	70

SUMMARY

This guidance provides airports with a comprehensive framework for evaluating, planning, implementing, and managing full employee screening programs. The research addresses the complex considerations airports face when determining whether full employee screening is appropriate for their unique circumstances. Successful full employee screening programs share several key elements:

- Comprehensive needs assessment and risk-informed business case development that justify investment
- Clear program scope definition with appropriate stakeholder engagement
- Strategic infrastructure planning and technology selection that support operational efficiency
- Well-designed prohibited items policies and operating procedures that maintain security while respecting operational realities
- Effective workforce management, training, and quality assurance systems
- Regulatory compliance and legally defensible procedures

Airports that implement these strategies effectively can achieve significant benefits:

- Enhanced security posture through proactive insider threat mitigation
- Reduced vulnerability to exploitation of access privileges
- Operationally sustainable programs that balance security requirements with business operations
- Enhanced preparedness for potential future regulatory developments
- Stronger stakeholder relationships built on transparent communication and collaborative implementation

Each airport faces unique circumstances requiring tailored approaches to full employee screening implementation. This guidance provides a practical framework for decision-making that enables airports to develop effective, sustainable, and legally defensible programs, while recognizing that full employee screening represents one important layer in a comprehensive security strategy.

PARAS ACRONYMS

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

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ADA	Americans with Disabilities Act
AIT	Advanced Imaging Technology
ASAC	Aviation Security Advisory Committee
ASP	Airport Security Program
ATL	Hartsfield-Jackson Atlanta International Airport
AWS	Aviation Worker Screening
DFW	Dallas-Fort Worth International Airport
ETD	Explosive Trace Detection
GSA	General Services Administration
ICAO	International Civil Aviation Organization
MII	Majority-in-Interest
NA	National Amendment
QR	Quick Response
RCA	Root Cause Analysis
RFI	Request for Information
RFQ	Request for Quotation
SLA	Service Level Agreement
WTMD	Walk-Through Metal Detector

SECTION 1: INTRODUCTION AND CURRENT IMPLEMENTATION LANDSCAPE

This section establishes the foundation for understanding full employee screening at airports by examining both the security imperatives driving consideration of these programs and the diverse implementation approaches currently employed across the industry.

The threat posed by aviation insiders—those with access to aircraft or sensitive areas—remains a significant security concern for airports of all sizes. In response, full employee screening has emerged as a potential strategy to enhance airport security and mitigate insider threats.

The movement toward enhanced employee screening in the United States also reflects evolving international standards. In 2019, the International Civil Aviation Organization (ICAO) adopted revised standards requiring member states to screen persons other than passengers, using methods capable of detecting explosives, applied either continuously or unpredictably before entry into security-restricted areas. While the United States filed an official difference to these standards, asserting that its multiple layers of security achieve equivalent outcomes, the adoption of these international requirements has influenced TSA's policy direction. TSA's 2023 National Amendment (NA) establishing Aviation Worker Screening (AWS) requirements represents a step toward enhanced screening of airport workers, although it stops short of the screening contemplated by ICAO standards. *For detailed discussion of ICAO standards, international agreements, and their regulatory implications, see Section 12.*

This research gathered comprehensive information about full employee screening practices, implementation challenges, and operational considerations across the US airport system. The methodology included an extensive review of relevant publications, government documentation, and industry resources, as well as comprehensive interviews with representatives of both US and international airports. Seven focus group discussions were conducted with airports of varying sizes and locations, gathering perspectives from those in different stages of employee screening implementation—from airports meeting baseline TSA AWS requirements to those operating comprehensive full screening programs. Five additional in-depth targeted interviews with airport security personnel, operations managers, and executive leadership provided detailed information about specific screening programs, implementation strategies, successful practices, and lessons learned. This multifaceted approach collected diverse perspectives that informed the practical guidance presented throughout this document.

Understanding "Full" Employee Screening Terminology

Throughout this report, "full employee screening" refers to programs that screen nearly all airport workers prior to entering security-restricted areas, while allowing for limited, formally managed exemptions for certain personnel such as law enforcement officers and actively responding first responders. This distinction between "full" and "100 percent" screening, where the latter would allow no exceptions whatsoever, is drawn from the Aviation Security Advisory Committee's (ASAC) definitions and is important for understanding the practical implementation approaches discussed throughout this report.¹ Additionally, many airports implement full employee screening through phased approaches, progressively expanding coverage based on infrastructure availability, operational learning, and resource constraints rather than implementing comprehensive screening simultaneously across all access points. *For foundational definitions and detailed discussion of program scope decisions, see Section 4.*

¹ ASAC, Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control (Washington, DC: Transportation Security Administration, April 8, 2015), 10.

1.1 Current State of Employee Screening Implementation

The PARAS 0063 research project conducted comprehensive interviews with airport representatives of US to understand current employee screening implementation strategies. This analysis highlights the variety of screening methods in use, from airports that only meet the TSA AWS requirements to those that have implemented comprehensive full employee screening programs.

1.1.1 Implementation Approaches

Before examining implementation patterns by airport category, it is important to understand the three primary approaches airports use for employee screening:

- **Full Employee Screening Program:** These programs require nearly all airport workers to be physically screened prior to entering security-restricted areas. Full employee screening is implemented by airports through three operational models:
 - **Airport-operated:** The airport directly manages and operates the screening checkpoints using either direct employees or contractors
 - **TSA-operated:** TSA operates dedicated employee screening checkpoints with federal personnel and equipment
 - **Hybrid:** Screening responsibilities are shared between multiple entities (TSA/airport-operated, TSA/airline/airport-operated), often with different operators covering different time periods or locations
- **AWS Only:** These airports meet regulatory obligations solely through the random, continuous screening required by the TSA AWS NA, without implementing any full employee screening checkpoints.
- **Partial/Mixed Implementation:** These airports apply full employee screening inconsistently across their facilities, such as implementing it in some terminals but not others, or at remote parking facilities but not at terminal access points.

1.1.2 Patterns by Airport Category

CATEGORY X AIRPORTS (MAJOR HUBS)

The 17 Category X airports studied showed the greatest diversity in implementation approaches:

- **Full Employee Screening Program:** 9 airports had implemented full employee screening:
 - Airport-Operated: 6 airports
 - TSA-Operated: 1 airport
 - Hybrid: 2 airports (1 TSA/airport hybrid, 1 TSA/airline/airport hybrid)
- **AWS-Only Program:** 5 airports operated AWS-only programs; 2 of these 5 airports were planning to implement full employee screening as part of upcoming terminal expansion or renovation projects.
- **Partial/Mixed Implementation Program:** 3 airports

CATEGORY I AIRPORTS (REGIONAL)

The 7 Category I airports studied demonstrated different patterns:

- **Full Employee Screening Program:** 1 airport had implemented full employee screening (airport-operated)

- **AWS-Only Program:** 6 airports had implemented AWS. However, 4 of these airports were planning to implement full employee screening as part of upcoming terminal expansions or renovations.

CATEGORY II AIRPORTS (SMALLER)

Both Category II airports studied implemented AWS-only programs, and neither airport had plans for full employee screening implementation.

Table 1 presents the implementation status, future plans, and staffing model for each of the 26 US airports interviewed for this research.

Table 1. Employee Screening Implementation Status

Category	Current Status	Future Plans	Staffing Model
X	AWS Only	Maintaining current program	Contract
X	AWS Only	Full employee screening planned (2026)	Contract
X	Full Employee Screening (Airport-operated)	Maintaining current program	Hybrid
X	Partial/Mixed Implementation	Full employee screening planned (2025)	Contract
X	Full Employee Screening (Airport-operated)	Maintaining current program	Contract
X	Full Employee Screening (Hybrid TSA/Airline/Airport)	Maintaining current program	Contract
X	Partial/Mixed Implementation	Maintaining current program	Contract
X	Full Employee Screening (Airport-operated)	Maintaining current program	Contract
X	AWS Only	Maintaining current program	Contract
X	Full Employee Screening (Airport-operated)	Maintaining current program	Contract
X	Full Employee Screening (Hybrid TSA/Airport)	Maintaining current program	Contract
X	Partial/Mixed Implementation	Maintaining current program	Contract
X	Full Employee Screening (Airport-operated)	Maintaining current program	Contract
X	AWS Only	Maintaining current program	Contract
X	AWS Only	Full employee screening under consideration	Contract
X	Full Employee Screening (Airport-operated)	Maintaining current program	Direct Employee
X	Full Employee Screening (TSA-operated)	Not specified	Contract
I	AWS Only	Not specified	Direct Employee
I	AWS Only	Full employee screening planned (2029)	Contract

Category	Current Status	Future Plans	Staffing Model
I	Full Employee Screening (Airport-operated)	Maintaining current program	Contract
I	AWS Only	Full employee screening planned	Contract
I	AWS Only	Full employee screening planned (2028)	Hybrid
I	AWS Only	Full employee screening planned (2025)	Contract
I	AWS Only	Not specified	Direct Employee
II	AWS Only	Not specified	Contract
II	AWS Only	Not specified	Direct Employee

1.2 Strategic Insights

The comprehensive analysis of the US airports in this report demonstrates that employee screening approaches are shaped by multiple factors. These include security imperatives, operational realities, and resource constraints. While the TSA AWS NA established a baseline standard for random continuous physical screening of airport workers at secure area access points, airports studied are charting divergent paths toward enhanced security based on their unique circumstances, risk profiles, and strategic priorities. These varied approaches to implementing employee screening, whether using full or hybrid models, offer valuable lessons for the domestic aviation security community as it navigates the evolving threat landscape and seeks to mitigate the risks posed by insider threats.

DRIVERS FOR FULL EMPLOYEE SCREENING IMPLEMENTATION

Historical security incidents and insider threat awareness: Recent high-profile airport smuggling cases have fundamentally shifted industry perspectives on insider threats, demonstrating how employees with legitimate access can exploit security vulnerabilities. These incidents have served as catalysts for full employee screening programs, with security leaders recognizing that reactive measures following breaches can be far more costly than proactive prevention strategies.

New terminal construction and major renovations: Several airports in the study had, or were planning to, strategically integrate full employee screening infrastructure into new terminal projects, avoiding costly retrofits while designing optimal screening layouts from inception. This approach allows airports to incorporate dedicated space, appropriate utilities, and efficient traffic flow patterns that would be challenging to achieve in existing facilities. *For detailed guidance on integrating employee screening infrastructure with capital projects, see Section 6.*

Proactive security posture and risk mitigation: Leading airports among those interviewed are moving beyond compliance-driven approaches to embrace full employee screening as a critical layer in their security program. These facilities recognize that the cost of a single security breach could have catastrophic consequences.

BARRIERS TO FULL EMPLOYEE SCREENING IMPLEMENTATION

Infrastructure constraints in aging terminals: Older airports face significant challenges to retrofitting screening checkpoints into spaces that were never designed for security operations, including structural limitations, inadequate electrical or data capacity, and compliance with Americans with Disabilities Act

(ADA) requirements. Several Category X, I, and II airports in our study reported that their existing terminal configurations could not accommodate the space requirements for screening equipment, queuing areas, and alarm resolution zones without major reconstruction.

Resource limitations and competing priorities: Smaller airports surveyed struggle to justify the staffing costs, equipment purchases, and infrastructure investments required for full employee screening when facing limited budgets and competing capital projects. The annual operational costs for full employee screening would represent significant ongoing commitments that would have to be coordinated with broader security and operational priorities.

Operational challenges for smaller airports: Category II airports face unique operational complexities due to employees performing multiple roles that also require frequent transitions between public and secure areas throughout their shifts. With limited staffing flexibility, these airports cannot easily absorb screening delays without impacting critical functions such as customer service, baggage handling, and aircraft servicing. The constant movement of multi-role employees between areas creates logistical challenges that larger airports with specialized staff may not experience.

Maintaining efficient employee traffic flow: Maintaining efficient employee traffic flow during shift changes while conducting thorough screening requires careful planning and sufficient infrastructure to avoid creating bottlenecks that may impact flight operations. Peak periods can generate substantial queuing in a short timeframe, and delays in screening can cascade into operational disruptions when employees cannot reach their work areas on schedule. Airports with high volumes of employees who frequently transition between public and secure areas throughout the day face particular challenges in maintaining consistent throughput without compromising screening effectiveness.

Stakeholder resistance and cultural change management: Implementation often faces initial resistance from airlines, tenants, and employees accustomed to unrestricted access, requiring sustained communication and education efforts to build acceptance. Several airports in the study reported that achieving cultural buy-in took 12–18 months of consistent engagement, with success dependent on clearly articulating security benefits and maintaining transparent dialogue about operational impacts.

1.3 Emerging Trends

Beyond the current drivers and barriers shaping implementation decisions, the research revealed five significant trends that are influencing how airports approach employee screening programs. These emerging patterns reflect the industry's evolution toward more strategic, collaborative, and technology-enabled security solutions.

1. **Integration with major construction projects:** The airports studied increasingly recognize that terminal renovations or expansions provide once-in-a-generation opportunities to incorporate screening infrastructure at significantly lower costs than standalone retrofits. This trend includes using design-build contracts that maintain flexibility for adjustments based on operational feedback during implementation phases. *For detailed guidance on integrating screening infrastructure with capital projects, see Section 6.*
2. **Hybrid staffing models gaining adoption:** Interviewed airports are finding success with models that combine direct airport employees for supervisory positions with contracted staff for screening operations, balancing control with flexibility. This approach allows airports to maintain oversight and quality standards while leveraging contractors' specialized expertise and ability to scale staffing based on operational demands.

3. **Technology enhancement and automation focus:** Implementation of AI-enhanced equipment, integrating biometric technology with airport access control systems, and networked monitoring systems reflect the industry's push toward security technologies that can improve both security effectiveness and operational efficiency.
4. **Airport-airline collaboration models:** One major airline's operation of 54 screening checkpoints across 15 airports demonstrates how airlines can partner with airports to implement comprehensive programs that align security objectives with operational needs. This collaborative approach, particularly evident at remote parking facility screening operations, shows how stakeholders can share responsibilities and resources to achieve common security goals.
5. **Risk-based and data-driven deployment strategies:** The airports surveyed are increasingly using access control data analytics to optimize checkpoint placement and staffing levels based on actual traffic patterns rather than assumptions about employee movement. This evidence-based approach helps airports justify infrastructure investments to stakeholders while ensuring resources are deployed where they provide maximum security value.

The diversity of approaches, ranging from AWS-only compliance to comprehensive full employee screening programs, reflects the complex alignment airports must achieve among security enhancement, operational efficiency, and resource management. This diverse implementation landscape provides essential context for airports considering their own screening programs

SECTION 2: NEEDS ASSESSMENT AND BUSINESS CASE

The decision to implement full employee screening represents a significant strategic and financial commitment. Before proceeding, airports must evaluate whether such a program is warranted for their specific circumstances and, if so, build a compelling case for executive approval and resource allocation. This section examines the analyses required to determine whether full employee screening is appropriate for a given airport.

2.1 Understanding the Need and Building the Business Case for Full Employee Screening

The process of determining whether to implement full employee screening involves multiple analytical and decision-making frameworks, including needs assessments, risk assessments, cost-benefit analyses, and business case development. Airports must first conduct risk assessments to understand their specific vulnerabilities and threat landscape. This assessment informs a cost-benefit analysis that weighs the financial investment required against the security enhancements and other potential benefits. The business case development process must also consider alternative approaches to addressing insider threats, recognizing that full employee screening represents one option among several strategies.

The assessment process must reconcile multiple competing factors. Security enhancement objectives must be weighed against operational impacts, including potential delays in employee processing and effects on workforce productivity. Airports must also consider how a full employee screening program fits within their broader security strategy, ensuring that resources are allocated effectively across multiple security layers.

2.1.1 Needs Assessment

A needs assessment is the formal, systematic process of identifying a performance gap or specific problem before committing resources to a solution. In the context of airport security, this process moves the conversation from general concerns about insider threats to a documented, specific, and data-supported problem statement. It answers the fundamental question: “What is the problem we are trying to solve, and how do we know it’s a real problem?” For airports considering full employee screening, a needs assessment provides the framework for proactive decision-making by identifying and defining security vulnerabilities before they are exploited.

ANALYTICAL TOOL: NEEDS ASSESSMENT

A formal process to identify and validate performance gaps before allocating resources. Establishes the “why” before exploring the “how” or “what” of potential solutions.

Key Resources:

- PARAS 0011: *Guidance for Airport Security Master Planning* – provides a holistic framework for long-term strategic security planning at airports.² It positions the needs assessment as an integral part of an ongoing, strategic security management cycle that should include two key activities:
 1. **Identifying Drivers and Strategy:** This involves defining the high-level strategic goals that the security initiative is intended to address. For full employee screening, this would require the airport to articulate what specific security gaps it is trying to close.
 2. **Airport Security Department Needs Assessment:** This is a more focused analysis that evaluates the current capabilities, resources, and requirements of the airport security organization itself.
- The DHS Interagency Security Committee guide, *Best Practices for Planning and Managing Physical Security Resources* (DHS, 2015), provides a framework for determining resource requirements based on operational needs.³ The framework was designed for federal facilities but is adaptable to airports.

Quick Application: Define specific security gaps, not general concerns. Document the problem systematically before evaluating solutions.

A critical function of the needs assessment is to properly scope the problem to avoid “solutioneering,” a common pitfall where a preferred solution is identified before the problem is fully understood. Insider threat is not monolithic; it encompasses many things, including drug trafficking, money laundering, firearms smuggling, and human trafficking. Therefore, a well-executed needs assessment should not begin with “Do we need full employee screening?” Instead, it should ask: “What is the nature, scale, and scope of our vulnerability to the illicit transport of goods, currency, and weapons by insiders?” This approach considers a full spectrum of potential solutions, with full employee screening as just one of several security strategies.

2.1.2 Risk Assessment

A risk assessment involves the systematic evaluation of threat identification and vulnerability assessment, analysis of potential consequences of security breaches, review of existing security measures and their effectiveness, and examination of intelligence and threat information from various sources. A comprehensive risk assessment can provide the foundation for determining whether full employee screening is appropriate for an airport.

For airports, a risk assessment translates abstract concerns into specific, prioritized scenarios. It helps move from the general knowledge that, “we have an insider threat problem” to a specific, actionable understanding, such as: “The most significant insider risk to our facility is an employee smuggling plastic explosive into an airport secure area and placing it onboard an aircraft where it detonates. A successful attack using this vulnerability could result in catastrophic loss of life, a multi-day airport closure with national economic impact, and irreparable damage to public confidence.” This level of specificity allows for the prioritization of risks and the targeted allocation of finite security resources to the most critical areas. It provides the essential, data-driven foundation upon which a credible cost-benefit analysis and a defensible business case can be built.

² National Safe Skies Alliance, Inc., *Guidance for Airport Security Master Planning*, PARAS 0011 (January 2019), 15-17.

³ U.S. Department of Homeland Security (DHS), *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide* (Washington, DC: DHS, 2015), 9.

ANALYTICAL TOOL: RISK ASSESSMENT

Risk assessment is a structured process to identify potential threats, assess vulnerabilities, and analyze consequences. The formula $\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Consequence}$ helps quantify security gaps and prioritize resources.

Key Resource:

- PARAS 0016: *Airport Security Vulnerability Assessments* – Provides a comprehensive, step-by-step methodology for conducting a Security Vulnerability Assessment, specifically for airports.⁴ The guidebook's 8-step process offers a clear, repeatable framework that is specifically tailored to the airport environment.

Quick Application: Begin by assembling a multidisciplinary team, review historical incident data focusing on patterns, analyze access control data to identify high-traffic points, and document findings formally to support business case development.

For detailed methodology, see PARAS 0016 Table 3-1⁵

It is critical to recognize that the goal of a risk assessment in a security context is not to predict the future with absolute certainty. Given the high degree of uncertainty surrounding terrorist threats and capabilities, complex predictive models should be used with caution. Their value lies not in generating a definitive probability of an attack, but in helping decision-makers “better understand the components of terrorism risk and to explore possible influences of system changes on that risk.”⁶ The assessment is a tool to support more informed, defensible decisions under conditions of uncertainty.

Many airports implementing full employee screening did so reactively in response to specific incidents rather than proactively based on comprehensive risk assessments. Decision-making was primarily driven by security breaches at the facility or industry-wide incidents. Only a few airports reported conducting formal threat and vulnerability assessments prior to implementation. This reactive pattern, while understandable given the incident-driven nature of aviation security, represents a missed opportunity for more strategic resource allocation and stakeholder engagement.

2.1.3 Root Cause Analysis

Root Cause Analysis (RCA) is another valuable tool for investigating persistent vulnerabilities, adverse events, or security failures to uncover underlying causes. This approach involves examining not just immediate security gaps but underlying systemic issues that create vulnerabilities. It functions as a diagnostic tool that moves beyond addressing the immediate, obvious symptoms of a problem. An RCA investigation drills down through layers of causality to find the fundamental, systemic origins of an issue. The primary value of RCA is that it helps airports develop targeted solutions that address core problems rather than merely patching the symptoms, thereby preventing the same failures from recurring.⁷

⁴ Mark Crosby, Michael Steinle, Kori Nobel, and Theresa Smith, *Airport Security Vulnerability Assessments*, PARAS 0016 (National Safe Skies Alliance, Inc., June 2020), 12.

⁵ Ibid.

⁶ Andrew R. Morral et al., *Modeling Terrorism Risk to the Air Transportation System: An Independent Assessment of TSA's Risk Management Analysis Tool and Associated Methods* (Santa Monica, CA: RAND Corporation, 2012).

⁷ McGee, Sibel, Ph.D. (PI), Peggy McCarthy, and Analytic Services Inc. (ANSER). *Guidance for Root Cause Analysis in Aviation Security (PARAS 0027)* (Falls Church, VA: National Safe Skies Alliance, January 2021), 8.

ANALYTICAL TOOL: ROOT CAUSE ANALYSIS

RCA is a diagnostic methodology that moves beyond symptoms to uncover fundamental causes of security vulnerabilities. By repeatedly asking “Why?” RCA drills down through causality layers to find systemic origins of issues.

Key Resource:

- PARAS 0027: *Guidance for Root Cause Analysis in Aviation Security* – Provides a complete 6-step methodology for conducting a RCA using techniques for drilling down from symptoms to causes.⁸ It is designed to be scalable for both simple and complex airport security issues.⁹

Quick Application: When a vulnerability is identified, assemble a team to map cause-effect relationships, identify leverage points where interventions will have maximum impact, and focus on systemic fixes rather than individual blame.

In the airport security environment, RCA provides critical diagnostic depth. If a risk assessment identifies *what* the key risks are (e.g., the risk of undetected contraband), RCA helps explain *why* those risks exist and persist. For example, if covert testing reveals that a checkpoint repeatedly fails to detect prohibited items, the symptom is “screening failure.” A superficial response might be to retrain or discipline the individual screener. An RCA, however, would investigate the systemic reasons *why* the failure occurred. Was it a result of inadequate initial training standards, poorly maintained or calibrated equipment, a flawed random selection process that became predictable, or a systemic cultural issue where operational throughput is implicitly prioritized over security effectiveness?

2.1.4 Cost-Benefit Analysis

Cost-benefit analysis (CBA) is a financial analysis technique used to evaluate the merits of a proposed project by comparing total expected costs against total expected benefits. The analysis involves identifying all potential costs and benefits, quantifying them in monetary terms to the greatest extent possible, and comparing them to determine if the project represents a sound investment. Results are typically expressed as a Benefit-Cost Ratio (where values greater than 1.0 indicate benefits exceed costs) or as Net Present Value, which calculates the total value in today’s dollars.

⁸ Ibid., 14–15.

⁹ Ibid., 2.

ANALYTICAL TOOL: COST-BENEFIT ANALYSIS

A systematic comparison of total expected costs against total expected benefits, quantified in monetary terms where possible. Provides decision-makers with a financial baseline to evaluate whether full employee screening represents a sound investment compared to alternatives.

Key Resources:

- The ISC guide, *Making a Business Case for Security: An Interagency Security Committee Best Practice* (DHS, 2023), provides a framework for identifying both quantitative and qualitative benefits and analyzing all required security investments.¹⁰ The guide also includes a downloadable Cost Analysis Template.¹¹
- The U.S. Government Accountability Office, *GAO-09-3SP: Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, provides a comprehensive framework and a detailed set of best practices for developing the 'cost' side of the CBA equation.¹² While this federal guide provides extensive detail that may exceed many airports' needs, its core principles and checklists offer valuable structure for any cost analysis.

Quick Application: Document all life cycle costs (capital and operational) over 10+ years. Focus benefits on measurable items (theft reduction, avoided investigations) rather than attempting to monetize catastrophic events. Consider breakeven approach for more concrete decision-making.

For airports considering full employee screening, CBA provides a disciplined, data-driven method for assessing financial and economic viability. It requires a thorough accounting of all costs, including equipment procurement as well as long-term expenses such as staffing, training, maintenance, and potential operational impacts. Simultaneously, it requires rigorous attempts to quantify benefits, including direct financial gains from reduced theft and the monetized value of avoided losses from security incidents. While quantifying the benefit of preventing incidents presents challenges, the structured CBA process provides decision-makers with a clear financial baseline to compare the proposed investment against alternatives or the status quo. The primary value of conducting a CBA in security contexts may lie less in the final numerical result than in the process itself. This systematic approach often uncovers hidden costs, forces crucial conversations about organizational priorities, and creates a transparent, well-documented foundation for decisions.

2.1.5 Business Case Development

Business case development is the process of creating a comprehensive document that provides full justification for undertaking a significant project or investment. It establishes a structured framework for answering key questions for executive decision-makers: What problem are we addressing? What are the viable options? For each option, what are the detailed costs, benefits, risks, and strategic implications that will inform the decision? What is the recommended course of action, and why is it superior to alternatives? For airports, a well-developed business case elevates a security proposal into a strategic business proposition, serving as the primary vehicle for securing executive, board-level, and stakeholder approval and funding.

¹⁰ ISC, *Making a Business Case for Security: An Interagency Security Committee Best Practice*, 2023 ed. (Washington, DC: DHS, 2023), 7.

¹¹ ISC, *Cost Analysis Template*, Excel spreadsheet (Washington, DC: DHS, 2023), https://www.cisa.gov/sites/default/files/2023-02/ISC_Making_a_Business_Case%E2%80%9393Cost_Analysis_Template.xlsx.

¹² U.S. Government Accountability Office, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, GAO-20-195G (Washington, DC: U.S. Government Accountability Office, 2020), 32.

ANALYTICAL TOOL: BUSINESS CASE DEVELOPMENT

A business case is a comprehensive document that establishes the framework and structure for justifying investment decisions and securing funding approval. The business case will integrate needs assessment, risk assessment, and cost-benefit analysis data once those analyses are complete.

Key Resources:

- *PARAS 0011* outlines several key principles that should inform the business case: solutions must be technically sound and flexible, they must meet the goals of all key stakeholders, and the full life cycle costs and training implications of new technology must be thoroughly understood.¹³
- The US Government Accountability Office's *Leading Practices: Agile Portfolio Management and Iterative Business Cases Drive Innovative Product Development* analyzes how leading commercial companies manage complex development efforts.¹⁴ It introduces an iterative approach that treats the business case as a living document that is systematically reassessed and updated as more knowledge is gained, making it well-suited for complex, high-uncertainty projects like the establishment of a new full employee screening program.¹⁵
- The ISC guide *Best Practices for Making a Business Case for Security* provides a structured approach to developing the rationale for an investment and weighing the benefits, costs, and risks of a solution against alternative options.¹⁶

Quick Application: Combine problem definition, alternative analysis, benefits articulation, and cost projections into a compelling narrative for airport executives.

A comprehensive business case for full employee screening requires multiple elements: detailed security impact assessments that quantify specific vulnerabilities, financial projections extending across the full equipment life cycle (typically 10–15 years), systematic evaluation of alternative security measures and their relative cost-effectiveness, and clear articulation of both quantifiable and intangible benefits. These components, especially the cost-benefit analysis discussed in the following section, provide the data and evidence needed to populate the business case framework. When properly developed, such a business case transforms what might otherwise be perceived as a reactive security mandate into a strategic investment decision, providing executives and stakeholders with the transparent, data-driven foundation necessary to justify the substantial financial, operational, and organizational commitments that full employee screening requires.

2.2 Key Findings

International aviation security organizations have recognized insider threats as a matter requiring robust security measures for worldwide implementation. The research revealed that the potential threat posed by insiders—those with access to aircraft or sensitive areas—has been a long-standing concern to international civil aviation security authorities. This recognition has led to evolving standards and recommendations for employee screening practices globally.

2.2.1 Security Incidents as Implementation Drivers

Security incidents consistently emerged as primary catalysts for program development among airports with full screening programs. These incidents included discoveries of smuggling operations during

¹³ National Safe Skies Alliance, *PARAS 0011*, 9.

¹⁴ GAO, *Leading Practices: Agile Portfolio Management and Iterative Business Cases Drive Innovative Product Development*, GAO-25-107130 (Washington, DC: GAO, 2025), 4.

¹⁵ Ibid.

¹⁶ ISC, *Making a Business Case for Security*, 6.

federal investigations, arrests of multiple employees for security violations, and identification of systematic criminal activities within airport operations.

At Hartsfield-Jackson Atlanta International Airport (ATL) in 2014, an airline employee smuggled over 150 firearms through secure access points and onto commercial flights by using his SIDA badge to bypass standard security checkpoints. Similarly, at Dallas-Fort Worth International Airport (DFW), between 2016 and 2018, a federal sting operation resulted in multiple airline employees using their positions to bypass security measures and smuggle what they believed was methamphetamine onto commercial flights, with one supervisor even agreeing to transport what he thought were plastic explosives.

The research identified that the high-profile incidents at ATL and DFW influenced multiple airports and at least one airline to either implement or seriously consider full employee screening programs. Congressional hearings following these incidents led to enhanced regulatory focus on insider threat mitigation and prompted many airports to reevaluate their security postures.

2.2.2 Proactive Implementation Approaches

The research identified several proactive approaches to program development. Some airports implemented screening after major airline partners raised concerns based on experiences at other locations. These airports recognized the potential for similar vulnerabilities and acted preemptively to address them. One airport implemented screening at remote employee parking lots as a pilot program without any specific incident prompting the decision.

Multiple airports incorporated screening infrastructure into major construction or renovation projects, even before determining whether to establish full screening programs. This forward-thinking approach allowed them to avoid costly retrofitting while maintaining flexibility for future security enhancements.

Some airports implemented employee screening programs proactively, anticipating potential regulatory changes from TSA. A Category X airport implemented full screening when a draft NA suggested mandatory requirements might follow, while a Category I airport established random screening after TSA's 2015 Information Circular indicated possible future requirements. Proactive implementation allowed these airports to develop programs on their own timelines while maintaining control over their approaches.

Several analytical processes and tools are available to help airports proactively assess whether full employee screening is appropriate for their specific circumstances. Rather than waiting for incidents to dictate security investments, airports can employ the structured frameworks discussed in Section 2.1 to identify vulnerabilities, evaluate options, and build defensible business cases before problems materialize. Each tool serves a distinct but complementary function in helping airports determine whether full employee screening is appropriate for their specific circumstances.

2.2.3 Full Employee Screening Program Costs

Airports in this research reported program costs that varied based on airport size, configuration, and implementation approach. Among airports that have implemented full screening, reported capital expenditures ranged from several million dollars for smaller operations to over \$25 million for one major Category X airport. These costs encompassed equipment procurement, infrastructure modifications, initial training and program setup, and technology integration with existing systems.

Operational costs included personnel expenses for screening staff, equipment maintenance and replacement, utilities and facility overhead, administrative and management costs, and ongoing training and quality assurance. Personnel costs typically represent the largest ongoing expense.

The research identified several factors that significantly influence program costs. Airport configuration and layout can dramatically affect infrastructure requirements, with some airports needing extensive modifications while others could adapt existing facilities. The choice between direct employees and contract security services has major cost implications, with each model presenting different financial profiles. Technology selection also proved critical, as airports reported that initial equipment costs can be misleading if ongoing operational expenses are not carefully evaluated.

Detailed implementation guidance is provided in subsequent sections of this report:

- *For detailed guidance on funding mechanisms and budget planning, see Section 3 Funding Considerations*
- *For guidance on screening technology evaluation, life cycle costs, and equipment maintenance considerations, see Section 7 Screening Technology*
- *For guidance on evaluating staffing approaches, including direct employees, contract personnel, and hybrid approaches, see Section 10 Workforce Management*

2.2.4 Infrastructure and Space Challenges

Physical infrastructure emerged as one of the most critical decision factors in determining the feasibility of implementing full employee screening. Four airports identified infrastructure or space availability among their top three considerations when evaluating full employee screening. Infrastructure frequently represented a significant barrier to implementation, with airports reporting challenges including limited space to create dedicated employee screening lanes and facility layouts that would require establishing screening at multiple separate locations. For airports facing such constraints, the complexity and cost of retrofitting numerous access points factored heavily into their assessment of whether full employee screening is appropriate for their current circumstances.

Airports considering or planning terminal construction or major renovation projects may find opportunities to incorporate screening infrastructure during the design and construction phases. Six airports incorporated or planned to incorporate screening infrastructure into terminal construction or renovation projects, reporting that this approach allowed them to avoid the higher costs associated with retrofitting existing facilities. Two airports reported including basic infrastructure provisions in capital planning—even before committing to full implementation—to preserve flexibility for future security enhancements.

When conducting infrastructure feasibility assessments, airports should consider three key decision points:

1. Determining whether existing facilities can accommodate screening without major structural modifications
2. Identifying opportunities for integration with upcoming capital projects
3. Evaluating whether the number and distribution of access points makes implementation operationally viable

Airports facing severe infrastructure constraints may conclude that alternative security measures represent more practical near-term approaches while monitoring for future facility modification opportunities.

For detailed infrastructure planning guidance including space requirements, utility specifications, checkpoint placement strategies, and construction considerations, see Section 6 Screening Infrastructure.

2.2.5 Executive Leadership and Organizational Culture

The research identified executive leadership support as a critical success factor for full employee screening programs. Airports that successfully implemented programs reported that obtaining C-suite understanding of security benefits and future requirements was essential for securing adequate funding and organizational commitment. One participant emphasized that airports must be willing to “own the safety and security of their passengers” rather than viewing it solely as a federal government responsibility.

Cultural differences in security approaches emerged as a significant theme. Internationally, many countries have implemented mandatory full employee screening for years, encountering minimal resistance and achieving broad compliance. In contrast, many domestic airports in the United States have remained skeptical of the need for, and have resisted implementing, full employee screening. Research participants noted that this difference reflects differences in concern for costs and operational impacts, as well as broader variations in security culture between domestic and international operations.

2.3 Recommendations and Implementation Guidance

1. BEGIN WITH A COMPREHENSIVE NEEDS ASSESSMENT

Establish a formal process to identify and validate specific security gaps before committing to any solution, including full employee screening.

Implementation Guidance: Start by defining the specific problem, not the solution. Detail what security vulnerabilities exist at your airport through systematic analysis rather than assumptions. Assemble a cross-functional team to examine historical incident patterns, access control data, and intelligence reports. Focus on articulating the nature, scale, and scope of insider threat vulnerabilities. Document findings formally to establish the “why” that will drive all subsequent analysis. Avoid solutioneering by keeping the assessment solution neutral. Use frameworks from PARAS 0011 to align the needs assessment with your airport’s strategic security objectives.

2. CONDUCT SYSTEMATIC RISK AND VULNERABILITY ASSESSMENT

Following identification of needs, evaluate specific threats, vulnerabilities, and potential consequences to prioritize security investments.

Implementation Guidance: Build upon the needs assessment by applying structured risk assessment methodologies. Use PARAS 0016’s 8-step process to systematically evaluate threats and vulnerabilities identified in your needs assessment. When vulnerabilities are identified, apply RCA to understand not just what gaps exist but also why they persist by examining systemic issues instead of focusing only on symptoms. Consider formally documenting risk levels using the $Risk = Threat \times Vulnerability \times Consequence$ formula. Engaging external consultants for an objective assessment can also be an effective option.

3. DEVELOP A COST-BENEFIT ANALYSIS APPROPRIATE TO YOUR AIRPORT’S SCALE

Conduct a systematic comparison of expected costs and benefits that match your airport’s resources and complexity.

Implementation Guidance: Start with a basic framework that can be expanded based on your airport's capabilities. At a minimum, document expected costs over 10 years, including equipment, infrastructure modifications, staffing (whether direct or contract), maintenance, and training. For benefits, focus on what you can estimate: potential reduction in theft losses, avoided investigation costs, and improved regulatory compliance positioning. Smaller airports can use simple spreadsheet templates and peer airport data for estimates. Larger airports may choose to develop more detailed analyses with multiple scenarios.

Key cost considerations all airports should capture include service level agreements (SLA) in procurement planning, comparison of contract versus direct employee options based on your governance structure, and infrastructure needs such as electrical upgrades.

For benefits, focus on practical metrics rather than trying to monetize catastrophic event prevention. Survey airports of similar size for their actual cost and benefit experiences. Document your analysis formally but tailor its depth to match your airport's decision-making needs. A clear and well-organized assessment is more useful than a complex analysis that is unlikely to be utilized.

4. BUILD A FORMAL BUSINESS CASE FOR EXECUTIVE APPROVAL

Synthesize all analyses into a comprehensive business case document that provides clear justification for the recommended approach.

Implementation Guidance: Integrate findings from your needs assessment, risk assessment, and CBA into a cohesive narrative. Structure the business case to address executive priorities: clearly articulate the problem being solved (from needs assessment), present risk levels and consequences (from risk assessment), provide detailed financial analysis with multiple scenarios (from CBA), analyze alternatives and explain why full screening is superior (or not), and include implementation timeline and resource requirements. Use iterative business case approaches that allow for updates as the program develops. Ensure the document is suitable for multiple audiences, including executives for approval, finance for funding, and stakeholders for buy-in. Frame full employee screening as a strategic investment rather than merely compliance.

5. ALIGN IMPLEMENTATION WITH INFRASTRUCTURE REALITIES

Integrate infrastructure assessment early in the planning process to determine feasibility and optimize implementation timing.

Implementation Guidance: Conduct an infrastructure feasibility assessment as part of the business case development. Evaluate whether existing facilities can accommodate screening without major modifications. Examine your Capital Improvement Plan for upcoming projects that could integrate screening infrastructure with minimal additional expense. Even if your airport is not committed to full employee screening, consider whether current or planned construction projects present opportunities to include basic infrastructure provisions that preserve flexibility for future security enhancements. For airports facing severe infrastructure constraints, acknowledge in the business case that alternative security measures may represent more practical near-term approaches.

For detailed infrastructure planning guidance including space requirements, utility specifications, and checkpoint placement strategies, see Section 6 Screening Infrastructure.

6. SECURE EXECUTIVE LEADERSHIP BUY-IN

Build leadership support appropriate to your airport's decision-making structure and size to drive program development and ensure adequate resources.

Implementation Guidance: Present your case for full employee screening in a way that matches your organization's formal decision-making processes, culture, and resources. Focus on clearly articulating the security need using findings from your needs assessment and risk analysis. Present your business case in terms relevant to your executives' priorities, such as risk mitigation and operational efficiency. Share examples from peer airports of similar size showing that full employee screening programs can be implemented with minimal to no disruption to airport operations. Consider arranging conversations and site visits to airports with successful programs, allowing your leadership to learn directly from similar organizations about their experiences and lessons learned.

SECTION 2 QUICK REFERENCE

- Conduct a formal needs assessment to validate specific security gaps before selecting solutions
- Apply systematic risk assessment and RCA to understand vulnerabilities
- Develop a cost-benefit analysis appropriate to your airport's scale and resources
- Build a formal business case synthesizing all analyses for executive approval
- Assess infrastructure feasibility early and align with capital improvement planning
- Secure leadership support through your organization's formal decision-making processes

SECTION 3: FUNDING CONSIDERATIONS

Securing adequate funding represents one of the most significant challenges for airports implementing full employee screening programs. Beyond initial capital investments, airports must plan for long-term operational sustainability and determine how costs will be allocated among stakeholders. This section examines the full scope of costs associated with full employee screening programs and the financial planning challenges airports face when pursuing implementation.

3.1 Understanding Program Costs and Funding Challenges

Launching a comprehensive full employee screening program at an airport demands significant financial commitment for both upfront capital costs and ongoing operational expenditures. Airports considering such programs must navigate various funding mechanisms, cost allocation models, and budget planning requirements while balancing competing priorities for limited resources. The financial commitment extends beyond equipment procurement to include staffing, training, maintenance, infrastructure modifications, and administrative overhead. Understanding the full scope of costs and available funding options is essential for developing a sustainable employee screening program that can maintain effectiveness over time without creating undue financial strain on airport operations or stakeholders.

Funding approaches among interviewed airports varied significantly based on governance structures, existing stakeholder agreements, and local financial conditions. Several airports successfully anticipated future requirements and added funding to their Capital Improvement Plans over multiple years, allowing unused funds to roll over and accumulate for eventual implementation. These diverse experiences provide valuable insights for airports evaluating how to structure and fund their employee screening programs while maintaining fiscal responsibility and operational efficiency.

3.1.1 Budget Planning and Cost Analysis

Thorough cost analyses proved essential before program implementation. Successful implementations relied on detailed financial models that captured key cost elements. These comprehensive approaches allowed for more accurate budget forecasting and helped prevent unexpected expenses during implementation. Key cost considerations identified include:

- Personnel expenses including wages, benefits, training, and equipment
- Costs for contract security staff, including contract management expenses and oversight
- Technology procurement and ongoing maintenance
- SLAs and extended warranty costs beyond manufacturer coverage
- Infrastructure modifications for screening checkpoints
- Administrative overhead and program management
- Consumable supplies and replacement equipment
- Utility costs for screening operations
- Throughput capacity requirements when selecting technology, which affect equipment quantity and the number of staffed screening lanes needed to meet demand

One airport emphasized that obtaining executive leadership buy-in and helping C-suite executives understand future requirements was critical for securing adequate funding.

3.1.2 Cost Allocation Models

The allocation of employee screening costs varied significantly among airports in the research based on governance structure and existing stakeholder agreements. The research identified three primary cost allocation approaches:

AIRLINE COST RECOVERY MODELS

Many airports in the study recover employee screening costs through airline rates and charges, with approaches varying based on airport governance structure and airline agreements. Several airports have formalized cost-sharing arrangements through different mechanisms. One airport obtained formal airline approval for their employee screening program, with airlines agreeing to help cover costs through existing rate structures. This approval process involved consultation with airline representatives and resulted in a formal agreement regarding cost allocation. Similarly, some airports allocate most employee screening costs to airlines, with one airport reporting that airlines cover 80–90% of screening program costs through this mechanism. A location-based approach is used by one airport that recovers contract security costs from carriers through a formula allocating expenses by facility type (airfield, terminals, other facilities), allowing more precise distribution of security costs based on where services are provided. Airports consistently emphasized that transparent communication about cost calculations and security benefits proved essential for gaining airline support, regardless of the allocation method chosen.

The most formal cost-sharing mechanism involves Majority-in-Interest (MII) approval.¹⁷ One major airport secured MII approval from airlines for their full employee screening program, with airlines helping cover both initial capital costs and ongoing operations and maintenance expenses through the established rate structure.

DIRECT AIRPORT FUNDING

Several airports interviewed fund employee screening entirely through their operating budgets without direct cost recovery from stakeholders. One airport reported initially using reserves to fund their program before incorporating costs into their annual budget for subsequent years. Another airport noted that its employee screening program is funded through their regular operating budget, with capital planning for equipment replacements and upgrades. One airport proactively anticipated screening requirements and added funding to their Capital Improvement Plan budget over several years, with unused funds rolling over annually. This airport's capital funding came from the general fund with no cost-sharing arrangements, though they are required to provide justification and obtain quotes for capital items, even when making immediate purchases.

TERMINAL OPERATOR RESPONSIBILITIES

In some cases, terminal operators are primarily responsible for implementing and funding employee screening programs. One airport noted that costs are primarily passed to terminal operators through lease agreements, with terminal operators responsible for implementing security programs in accordance with lease obligations. The exception was for terminals operated directly by the airport authority, which required direct funding from the operating budget.

¹⁷ MII provisions in airport-airline use and lease agreements require airlines representing a specified majority share of enplanements or lease commitments to approve certain capital projects before implementation. This mechanism ensures airline input on major expenditures since these costs are typically recovered through landing fees and terminal rates. MII approval indicates both airline consent and, often, their participation in funding the project through the airport's rate structure.

3.1.3 Funding Sources

Airports employ diverse funding mechanisms to support full employee screening programs, drawing from both capital and operational funding streams. The choice of funding sources depends on multiple factors including airport governance structure, bonding capacity, eligibility for federal programs, and whether costs are classified as capital improvements or operational expenses. Understanding the range of available funding options and their respective limitations enables airports to develop sustainable financing strategies that align with their specific circumstances and long-term planning objectives.

Capital Expenses

The airports involved in this study categorized various items as capital expenses for employee screening implementation. Initial equipment purchases including x-ray machines and metal detectors, infrastructure modifications for building or renovating screening checkpoints, technology for access control and surveillance, and initial training program development were commonly treated as capital expenditures.

Among the interviewed airports, one reported that their initial employee screening implementation, which cost over \$25 million, was treated as a capital project with associated depreciation schedules. This approach allowed them to spread the cost over multiple years rather than absorbing it entirely in the implementation year.

As mentioned in Section 1.2, multiple airports used terminal construction or renovation projects as an opportunity to integrate full employee screening requirements into these larger initiatives. One airport reported incorporating the infrastructure for employee screening during construction to avoid higher retrofit costs later. Supporting infrastructure for a full employee screening checkpoint typically includes electrical capacity for screening equipment, data connectivity for security system integration for access control, and physical space modifications to accommodate the employee queue, screening operations, and physical barriers to define a Sterile Area and preclude the ability to bypass the screening process. The airport established a separate capital project for screening equipment but built the supporting infrastructure elements into the larger project budget.

Operating Expenses

Operational expenses represent recurring costs necessary to maintain programs year after year. Airports in the study typically included staffing or contractor costs, equipment maintenance contracts, consumable supplies, ongoing training and recertification, and technology licenses as operational expenses.

The method of funding operational expenses varied among participating airports, with one airport incorporating ongoing operations and maintenance costs into its regular operating budget after the initial capital project was completed. Other airports recovered these ongoing costs from stakeholders; one major airport secured an MII agreement under which airlines covered both capital and operations and maintenance costs, and another passing costs to terminal operators through lease agreements. Several airports stressed the importance of securing both capital and operational funding before implementing employee screening, noting that failure to account for ongoing operational costs can lead to program sustainability issues.

AIRPORT REVENUE BONDS

Airport revenue bonds have historically been one of the primary mechanisms for financing capital projects at large US airports, often accounting for more than half of capital raised in certain periods. While the exact share varies by airport size and project time frame, bonds remain a central tool for

financing terminal expansions, renovations, and security-related infrastructure. Several types of bonds may be applicable for employee screening initiatives:

- General airport revenue bonds secured by revenues generated at the airport
- General obligation bonds backed by the general tax base, offering stronger credit and lower interest rates
- Special facility bonds used to finance facilities for specific tenants

While no airports in our study specifically reported using bond financing solely for employee screening, several mentioned incorporating screening facilities into larger bond-funded terminal projects.

FAA CAPITAL FUNDING PROGRAMS

The FAA administers two primary funding mechanisms that airports may consider for full employee screening infrastructure: the AIP and Passenger Facility Charges (PFC). While both programs support airport capital development, they differ in their eligibility criteria for security equipment. Understanding these distinctions is essential for airports developing funding strategies for full employee screening programs, as certain components may qualify under one program but not the other.

Airport Improvement Program

The AIP provides federal grants funded by aviation user taxes deposited in the Airport and Airway Trust Fund.¹⁸ AIP eligibility is governed by the statutory definition of “airport development” in 49 USC § 47102, which emphasizes infrastructure that is “acquired for, or installed at” a public-use airport.¹⁹ The FAA interprets this statutory language to favor fixed capital improvements over movable operational equipment, a distinction that significantly affects eligibility of AIP funds for full employee screening programs.

For security projects, the AIP Handbook (FAA Order 5100.38D) establishes that equipment must generally be approved by TSA in writing as necessary to meet the minimum requirements of 49 CFR § 1542.²⁰ Eligible security equipment categories include terminal access control systems, perimeter fencing, badging equipment, fingerprinting equipment for background checks, and CCTV systems for secure areas.²¹ Each category requires written TSA approval confirming the equipment meets regulatory requirements.

The AIP’s treatment of employee screening infrastructure and equipment reflects the broader “fixed versus movable” distinction that governs program eligibility. Fixed infrastructure components associated with screening checkpoints, including structural modifications, electrical capacity upgrades, data connectivity installations, and physical barriers defining airport secure areas, are generally eligible as terminal development.²² However, the screening devices themselves, such as x-ray machines for property inspection, walk-through metal detectors (WTMD), and advanced imaging technology (AIT) systems, are generally not AIP-eligible because they are classified as movable operational equipment rather than fixed capital improvements.²³ This effectively limits AIP funding to the checkpoint infrastructure while excluding the machines inside the checkpoint.

¹⁸ FAA, Airport Improvement Program (AIP) Handbook, FAA Order 5100.38D, Change 1 (Washington, DC: February 26, 2019), 1-1.

¹⁹ 49 U.S.C. § 47102(3)(B).

²⁰ FAA, *AIP Handbook*, L-19.

²¹ FAA, *AIP Handbook*, Table L-2, L-19 to L-20.

²² FAA, *AIP Handbook*, Table N-5, N-5 to N-6.

²³ The AIP Handbook notes that passenger screening areas have “limited eligibility” restricted to “the construction of bare space (drywall, standard paint, and standard floor covering) with appropriate utilities.” FAA, *AIP Handbook*, N-5

The rationale for this distinction stems from both statutory interpretation and jurisdictional considerations. Movable screening equipment has historically fallen within TSA's operational responsibility for passenger checkpoints, and the AIP is statutorily prohibited from funding airport operations.²⁴ Although employee screening checkpoints represent an airport responsibility rather than a TSA function, the FAA applies the same fixed-versus-movable framework to determine eligibility. Items that can be unbolted, relocated, or carried away are viewed as operational tools rather than permanent improvements to real property.

A notable exception to these restrictions emerged from the FAA Reauthorization Act of 2018, which expanded AIP eligibility for CCTV systems. Section 138 of the Act amended 49 USC § 47119 to permit AIP funding for the installation of security cameras in public areas of the terminal interior and exterior, extending eligibility beyond the cameras required by 49 CFR § 1542.²⁵ The FAA has interpreted this provision to include acquisition costs (not just installation) provided specific conditions are met.²⁶

To qualify for expanded CCTV funding under this provision, airports must satisfy two procedural requirements. First, the airport must obtain written confirmation from TSA declining to fund the requested cameras.²⁷ Second, cameras purchased with AIP funds must be owned and operated solely by airport personnel; the airport may not acquire cameras for TSA or airline use, although the camera feeds may support TSA and other municipal operations under mutual aid agreements.²⁸ A special grant condition documenting these certifications is incorporated into the grant agreement.²⁹ While this expansion applies specifically to CCTV rather than screening equipment, it demonstrates the procedural pathway through which certain security technologies can become AIP-eligible when TSA declines funding responsibility.

Passenger Facility Charges

PFCs provide airports with greater flexibility for funding security equipment than AIP grants. Under 49 USC § 40117, airports with FAA approval may collect up to \$4.50 per enplaned passenger for eligible capital projects that preserve or enhance safety, security, or capacity of the national air transportation system.³⁰ PFC revenues represent a meaningful share of airport capital funding; in fiscal year 2020, PFC collections totaled approximately \$2.1 billion alongside \$20.3 billion in capital expenditures nationally.³¹

The key distinction between PFC and AIP eligibility is that PFCs are not bound by AIP's fixed-versus-movable framework. Instead, PFC eligibility for equipment turns on standard accounting definitions: whether the item qualifies as a capital asset (useful life exceeding one year and acquisition cost meeting applicable capitalization thresholds) and serves an approved project objective such as enhancing

²⁴ 49 U.S.C. § 47102(3) defines "airport development" to exclude operational costs. The FAA interprets movable equipment used by airport staff as operational rather than capital in nature. See FAA, *AIP Handbook*, C-1 to C-14.

²⁵ FAA Reauthorization Act of 2018, Pub. L. No. 115-254, § 138, 132 Stat. 3186 (2018), amending 49 U.S.C. § 47119(a)(1)(B).

²⁶ FAA, *Updated Reauthorization Program Guidance Letter (R-PGL) 19-02: Planning and Project Eligibility* (Washington, DC: March 4, 2022), 7.

²⁷ FAA, R-PGL 19-02, 7.

²⁸ FAA, R-PGL 19-02, 7–8.

²⁹ The special grant condition states: "The sponsor hereby certifies it has requested TSA funding for security cameras outside the scope of the airport's 49 CFR part 1542 plan but TSA denied the request in writing... The sponsor further certifies cameras acquired and installed under this grant will be for the sole use of the airport sponsor and its personnel for airport purposes." FAA, R-PGL 19-02, 8.

³⁰ 49 U.S.C. § 40117(b)(4); FAA, "Passenger Facility Charge (PFC) Program," accessed January 15, 2026, <https://www.faa.gov/airports/pfc>.

³¹ FAA, *National Plan of Integrated Airport Systems (NPIAS), 2023–2027* (Washington, DC: September 2023), 15.

security.³² The AIP Handbook acknowledges this difference, noting that “because PFC eligibility is based on AIP eligibility, leaving the project eligible but prohibiting use of AIP still allows these projects to be funded with PFC funds.”³³ This provision was written in the context of explosive detection systems, where congressional appropriations riders prohibited AIP funding but PFC eligibility remained intact.

For employee screening programs, this distinction has practical significance. Because employee screening is typically an airport responsibility rather than a TSA function, the equipment costs fall to the airport rather than the federal government. PFC revenues may be applied to screening equipment purchases, including x-ray machines, WTMDs, explosive trace detection (ETD) systems, and other screening equipment, provided the project meets the statutory objective of preserving or enhancing security.³⁴ Infrastructure components such as checkpoint construction, utility modifications, and access control integration are also PFC-eligible, consistent with their AIP eligibility.³⁵

Airports considering PFC funding for employee screening equipment should document that the equipment serves an airport-controlled security function and that TSA has not assumed responsibility for the specific checkpoint or equipment.³⁶ Proper capitalization of equipment purchases is essential to document that PFC revenues were applied to allowable capital costs rather than operational expenses.³⁷ Equipment funded through PFCs should be recorded on the airport’s fixed asset register and tracked for its useful life in accordance with applicable accounting standards.

However, not all portions of an employee screening project will necessarily qualify for PFC funding. Operational expenses such as staffing costs, ongoing maintenance contracts, and consumable supplies (including ETD swabs and test materials) are ineligible because they do not meet the definition of capital costs.³⁸ Additionally, many airports have already committed substantial PFC revenues to debt service on existing infrastructure projects, which may constrain available funding for new initiatives.³⁹

Table 2 summarizes the general eligibility of employee screening program components under AIP and PFC funding.

³² The definition of equipment as a capital asset with useful life exceeding one year and per-unit acquisition cost meeting applicable thresholds derives from 2 CFR § 200.1. PFC project objectives are established in 49 U.S.C. § 40117(a)(3)

³³ FAA, *AIP Handbook*, N-6.

³⁴ 49 U.S.C. § 40117(a)(3)(A) authorizes PFC projects that “preserve or enhance safety, security, or capacity of the national air transportation system.”

³⁵ U.S. Government Accountability Office, *Airport Infrastructure: Information on Funding and Financing for Planned Projects*, GAO-20-298 (Washington, DC: February 2020), 11.

³⁶ Airports should document that equipment serves an airport security function under 49 CFR Part 1542 that TSA has not assumed responsibility for staffing or equipping.

³⁷ 14 CFR § 158.13 establishes allowable costs for PFC-funded projects.

³⁸ 14 CFR § 158.13 establishes allowable costs for PFC-funded projects, limiting eligibility to costs incurred for approved capital projects. Ongoing operational expenses such as staffing, maintenance contracts, and consumable supplies do not qualify as project costs under this regulation.

³⁹ According to FAA data, airports paid approximately \$12 billion (78 percent of total PFC revenues collected) for debt service during fiscal years 2013 through 2017. GAO-20-298, 32.

Table 2. AIP and PFC Eligibility for Full Employee Screening Program Components

Component	AIP Eligibility	PFC Eligibility	Notes
Checkpoint infrastructure (walls, floors, barriers)	Generally eligible	Eligible	Classified as terminal development; may require TSA written approval
Electrical capacity and data connectivity	Generally eligible	Eligible	Supporting infrastructure for screening operations
X-ray machines and property screening equipment	Not eligible	Eligible	Classified as movable operational equipment under AIP
WTMDs	Not eligible	Eligible	Classified as movable operational equipment under AIP
AIT	Not eligible	Eligible	Classified as movable operational equipment under AIP
ETD systems	Not eligible	Eligible	Desktop/portable devices classified as movable operational equipment
Access control systems and biometric readers	Generally eligible	Eligible	Requires TSA written approval for AIP; must meet 49 CFR § 1542
CCTV systems (secured areas)	Eligible	Eligible	Requires TSA written approval for AIP
CCTV systems (terminal public areas)	Eligible with conditions	Eligible	Requires TSA written declination; airport-only ownership (per 2018 FAA Reauthorization)
Identity management system integration	Generally eligible	Eligible	Software and middleware linking credentialing to access control
Staffing and personnel costs	Not eligible	Not eligible	Operational expense; neither program funds airport operations
Ongoing maintenance contracts	Not eligible	Not eligible	Operational expense
Consumable supplies (ETD swabs, test materials)	Not eligible	Not eligible	Operational expense
Ongoing training and recertification	Not eligible	Not eligible	Operational expense; initial training program development may qualify as capital

Note: Eligibility determinations are general guidance based on FAA policy documents. Airports should consult with their FAA Airports District Office and review current program guidance to confirm eligibility for specific projects.

OPERATING BUDGET REALLOCATION

Several airports interviewed reported initially reallocating funds from other departments or using reserve funds to implement employee screening. One airport described initially reallocating funds from other departments before eventually absorbing costs through their regular budget process. Similarly, another airport reported using reserves initially before adding employee screening as a line item in subsequent budget years.

PRIVATE AND AIRLINE-FUNDED MODELS

Some US airports and many abroad adopt privatized or airline-led terminal development approaches, using project-specific revenues to pay off construction debt. While no airports specifically reported

using this approach for employee screening, it represents a potential model where airlines or private developers fund specialized staff checkpoints through long-term agreements.

3.1.4 Cost Management Strategies

Beyond funding mechanisms and budget planning, airports employ numerous operational strategies to manage and reduce costs. These strategies are addressed within their relevant implementation contexts:

- **Access point consolidation and checkpoint design efficiencies** → See *Section 6 Screening Infrastructure* for guidance on optimizing the number and location of screening points, consolidating checkpoints for efficiency, and incorporating screening infrastructure into construction projects
- **Equipment lifecycle and maintenance strategies** → See *Section 7 Screening Technology* for detailed information on equipment redundancy planning, SLAs, preventive maintenance programs, and total cost of ownership considerations
- **Staffing optimization and contract management** → See *Section 10 Staffing Considerations* for comprehensive coverage of contractor versus direct employee models, flexible staffing strategies, contract structuring for cost control, and workforce efficiency measures

By integrating cost management strategies within their operational contexts, airports can better understand how financial decisions relate to practical implementation considerations.

3.2 Recommendations and Implementation Guidance

1. CONDUCT COMPREHENSIVE FINANCIAL ANALYSIS

Develop a detailed cost assessment that captures all direct and indirect expenses associated with implementing and maintaining a full employee screening program.

Implementation Guidance: Begin by creating a comprehensive spreadsheet or financial model that includes initial capital expenditures for equipment, infrastructure modifications, and training programs. Calculate projected ongoing operational costs including staffing at various coverage levels, maintenance contracts, utilities, and consumables. Consider quantifiable benefits such as potential reduction in security incidents and regulatory compliance. Assess the expected lifespan of screening equipment and infrastructure to plan for replacement cycles. When developing the assessment, engage security, operations, law enforcement, finance, and risk management departments to ensure all potential expenses are captured. Use data from airports of similar size and operational complexity to validate cost estimates where possible.

2. EVALUATE AND SELECT APPROPRIATE COST ALLOCATION MODELS

Assess available cost allocation approaches based on your airport's governance structure and stakeholder relationships to determine the most sustainable funding model.

Implementation Guidance: Review your airport's existing rate-setting methodology and agreements with airlines and terminal operators to identify opportunities for cost recovery. If considering airline cost recovery, prepare a detailed justification explaining security benefits and regulatory requirements to facilitate stakeholder buy-in. For airports with terminal operators, examine lease agreements to determine if security costs can be incorporated into existing structures or if amendments are needed. Consider a phased approach where initial costs might be absorbed by the airport with gradual transition to stakeholder cost-sharing. Document any cost allocation agreements formally to ensure long-term sustainability and avoid future disputes.

3. DISTINGUISH CAPITAL FROM OPERATIONAL EXPENSES

Properly categorize expenses as capital or operational to optimize funding sources and budget planning.

Implementation Guidance: Work with your finance department to establish clear criteria for capital versus operational expenses based on your airport's policies and applicable accounting standards. Typically, classify initial equipment purchases, infrastructure modifications, and major technology systems as capital expenses that can be depreciated over time. Include staffing, maintenance contracts, consumables, and recurring licenses as operational expenses in annual budgets. Consider incorporating employee screening infrastructure into larger capital projects when possible to achieve economies of scale. For airports anticipating future screening requirements, consider adding funding to Capital Improvement Plans over multiple years, allowing unused funds to roll over and accumulate. Even if not ready to purchase immediately, obtain quotes and justification for capital items to support budget requests and maintain funding allocations. Plan for the transition from capital project funding to operational budget support well before implementation to avoid funding gaps.

4. EXPLORE MULTIPLE FUNDING SOURCES

Investigate various funding mechanisms including traditional and innovative approaches to support your employee screening program.

Implementation Guidance: Evaluate whether employee screening infrastructure can be partially funded through AIP grants if it enhances overall airport security. Assess PFC eligibility for components that benefit public area security. Consider incorporating screening facilities into larger bond-funded terminal projects to spread costs across broader initiatives. For airports with strong airline partnerships, explore private funding models where stakeholders might invest in security infrastructure through long-term agreements.

SECTION 3 QUICK REFERENCE

- Conduct comprehensive financial analysis including all direct and indirect costs
- Select sustainable cost allocation model based on airport governance structure
- Properly distinguish capital from operational expenses for optimal funding
- Explore multiple funding sources including grants, bonds, and stakeholder partnerships
- Develop sustainable budget planning processes with dedicated line items

SECTION 4: PROGRAM SCOPE

Developing a comprehensive full employee screening program requires airports to make critical decisions about program scope that will shape the program's effectiveness, feasibility, and acceptance by stakeholders. These foundational decisions encompass defining screening boundaries, determining scalability requirements, planning implementation phases, and choosing screening strategies based on the airport's specific operational conditions.

4.1 Defining Program Scope and Screening Boundaries

Early decisions about screening boundaries, checkpoint locations, and exemption policies have lasting operational and financial consequences, making thorough analysis essential before committing resources. Airports face varying challenges based on their physical configurations, workforce populations, and operational patterns, requiring approaches tailored to local conditions. Among the airports interviewed, data-driven methodologies emerged as a common thread, with many using access control systems and employee movement analysis to inform their scope decisions.

Research with airports that have implemented full employee screening programs reveals critical insights across four fundamental areas of program scope: 1) how airports define and establish screening boundaries, both within terminals and across the broader airport environment; 2) how they design infrastructure and technology for scalability; 3) how they approach phased implementation to manage operational change; and 4) how they maintain program integrity through formal exemption management. Together, these elements form an integrated framework that airports must consider when determining the scope of their screening programs. Understanding these scope decisions begins with establishing clear definitions of the key regulatory areas and the concept of full employee screening itself.

FOUNDATIONAL DEFINITIONS FOR FULL EMPLOYEE SCREENING PROGRAMS

- **Full Employee Screening:** The practical application of comprehensive screening to nearly all airport workers prior to entering security-restricted areas, while explicitly allowing for a limited and formally managed set of exemptions for certain personnel, such as law enforcement officers and first responders actively responding to an emergency.⁴⁰
- **100 Percent Employee Screening:** A theoretical construct in which all airport workers are screened with no exceptions whatsoever. The ASAC draws a distinction between "full" and "100 percent" screening, recognizing that practical implementation requires limited exemptions for certain operational necessities.⁴¹
- **Phased Implementation:** An approach in which airports progressively expand full employee screening coverage over time, such as implementing at certain terminals or access points before expanding to others, rather than deploying comprehensive screening simultaneously across all locations.
- **Air Operations Area (AOA):** A portion of an airport, specified in the Airport Security Program (ASP), in which security measures are carried out. This area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas.⁴²
- **Secured Area:** A portion of an airport where aircraft operators enplane and deplane passengers and sort and load baggage, and any adjacent areas not separated by adequate security measures.⁴³

⁴⁰ GAO-21-273, "Aviation Security: TSA Could Strengthen Its Insider Threat Program by Improving Guidance and Oversight" (Washington, D.C.: Government Accountability Office, 2021); ASAC, Final Report of the Working Group on Airport Access Control, 10.

⁴¹ Ibid.

⁴² 49 CFR § 1540.5.

⁴³ Ibid.

- **Security Identification Display Area (SIDA):** A portion of an airport where security measures specified in 49 CFR § 1542 are carried out. This includes the Secured Area and may include other areas of the airport.⁴
- **Sterile Area:** The portion of an airport that provides passengers access to board aircraft and to which access is generally controlled through the screening of persons and property.⁵

4.1.1 Establishing Screening Boundaries

Full employee screening programs require airports to establish screening boundaries that encompass all major access points into airport SIDA and Secured Areas. Successful programs analyzed employee movement patterns through sophisticated access control data examination, identifying not just which access points to utilize but also when and how different employee populations move through the airport environment. This analysis revealed that airports implement screening through three primary operational models, each addressing different infrastructure and operational requirements.

TERMINAL-BASED SCREENING OPERATIONS

Most airports concentrate screening operations at strategic points within terminal buildings where employees transition from public areas into secure zones. These dedicated employee-only checkpoints are typically positioned at major access points leading to SIDA and Secured Areas, with several conducting multidimensional analyses of badge reader transactions across different times of day, days of week, and seasonal variations to optimize placement. For employees requiring access to Sterile Areas, many airports in our study utilize existing TSA passenger screening checkpoints rather than duplicating infrastructure. Physical layout significantly influences these decisions—older facilities constructed in the 1950s often lack suitable spaces for centralized checkpoints, while newer construction allows optimal placement of multi-lane screening facilities. Airports with vertical or multilevel terminal designs face unique challenges compared to horizontal layouts, often requiring creative solutions for checkpoint placement and queue management.

PERIMETER AND VEHICLE ACCESS SCREENING

Four airports interviewed have extended screening operations to perimeter vehicle gates, establishing inspection stations where both employees and their vehicles are screened before entering the AOA. These operations require substantial infrastructure investments including weather protection, utilities, staffing facilities, and inspection equipment. This approach, while resource-intensive, addresses vulnerabilities at service and delivery entry points where goods enter secure areas, and at construction access points that might otherwise create security gaps. However, one airport noted that vehicle gate screening proved infeasible due to traffic flow patterns and infrastructure limitations, highlighting that this approach requires careful site-specific evaluation.

REMOTE SCREENING WITH CONSOLIDATED TRANSPORT

Two innovative implementations involve screening employees at remote parking facilities before transporting them via secure shuttle to operations areas. One airport operates this system directly, while at another location an airline manages the remote screening facility for its employees. This model offers several advantages: reducing congestion at terminal and perimeter access points, consolidating screening operations for better resource utilization, and providing weather-protected screening environments. The approach requires careful coordination of shuttle schedules with shift patterns and flight operations to maintain operational efficiency.

ACCESS POINT CONSOLIDATION AND OPTIMIZATION

Regardless of the screening model chosen, airports in the study emphasized the critical importance of reducing total access points to improve both security effectiveness and resource allocation. Data from access control systems helped airports identify consolidation opportunities, with multiple facilities

successfully closing dozens of underutilized doors and concentrating resources at high-volume locations. This consolidation process involved mapping employee pathways through facilities, correlating patterns with flight schedules and shift changes, and evaluating usage patterns to distinguish essential from convenience-based access points. Some airports implemented bidirectional screening for both entry and exit, providing enhanced security and mitigation for loss prevention, but requiring additional resources and careful planning of checkpoint locations to avoid creating operational bottlenecks.

4.1.2 Scalability Considerations

Scalability, which refers to the ability to adjust a screening program's capabilities to match changing conditions, proves crucial for effective implementation. Research with airports of various sizes indicates that effective scalability planning addresses two key factors: infrastructure flexibility and technology capabilities.

- **Infrastructure Scalability:** Physical infrastructure must accommodate current needs and potential future expansion. Several airports interviewed purposefully incorporated scalability into planning by designing facilities with expansion capabilities, including space for additional lanes and equipment. *For detailed guidance on integrating employee screening infrastructure with capital projects, see Section 6.*
- **Technology Scalability:** Technology choices significantly influence scaling ability. Several airports interviewed reported selecting technologies based partly on scalability characteristics, with biometric verification reducing staffing needs and AI-enhanced x-ray technology with automated threat detection reducing screening time and increasing throughput. Future-ready systems offering software updates and modular enhancement capabilities allow performance improvements and expanded functionality without hardware replacement. Remote monitoring capabilities enable security personnel to oversee multiple screening locations, expanding coverage without proportional staffing increases. Equipment life cycle management through structured approaches to evaluation, maintenance, and replacement ensures continued capability while controlling costs.

4.1.3 Phased Implementation Approaches

Phased implementation allows gradual introduction or expansion of screening programs, providing time for adjustment, training, and refinement based on operational experience. Common implementation approaches involved phased deployment as employee checkpoints were built out and deployed. This approach allowed airports to evaluate procedures, train staff, and refine operations at each location before expanding to additional checkpoints. Implementation periods typically range from a few days to a few weeks prior to opening each employee screening checkpoint, providing stakeholders opportunities to experience the screening process firsthand while allowing personnel to practice procedures.

Integration with planned construction or renovation projects has proven to be particularly effective. A number of airports leveraged terminal renovation projects to implement screening infrastructure during construction, avoiding higher retrofit costs. This approach typically involved establishing separate capital projects for screening equipment while building supporting infrastructure into larger project budgets. Phased implementation also facilitated gradual closure or consolidation of access points, allowing concentration of resources on higher-volume locations.

Stakeholder communication and preparation emerged as critical components of phased implementation. One airport we spoke with developed a comprehensive approach including demonstrations of screening processes using actual equipment and clear explanations of new requirements. This approach helped

secure buy-in from the badged population before full implementation. Multiple airports emphasized the value of inviting stakeholders to observe portal operations during pilot phases, allowing hands-on demonstrations with actual equipment. This transparency helped address concerns and built acceptance while providing opportunities to refine procedures based on stakeholder feedback.

4.1.4 Managing Population Exemptions

Most airports surveyed follow TSA AWS NA criteria for exemption eligibility. Commonly exempt populations include law enforcement officers, firefighters, and emergency medical services personnel responding to active emergencies. Some airports in our study secured additional exemptions from local TSA authorities for non-first responders involved in urgent critical infrastructure maintenance or specialized personnel like USDA wildlife officers authorized to carry firearms. Establishing these exemptions requires detailed documentation, clear justification, and regular review.

- **Management Protocols:** Integrity was maintained through structured management protocols, which included formal application processes overseen by security departments and required senior leadership approval. Visual identifiers on badges facilitate quick recognition. Regular review and revalidation prevent exemption creep and ensure continued justification. Coordination with TSA on eligible exempt populations maintains continuous compliance.
- **Documentation and Tracking:** Comprehensive documentation in SOPs was emphasized as an important practice. Several airports maintain procedures for identifying exempt populations through regular badge inspections and documentation reviews. Advanced tracking systems monitor exempt badge usage patterns and flag anomalies for investigation, with quarterly reviews evaluating continued necessity and compliance.
- **Security Measures for Exempt Individuals:** Alternative security measures minimize risks associated with exemptions. Among the airports we spoke with, approaches include visual identification verification and badge inspections for exempt groups. Clear definition of exemption conditions, such as limiting exemptions to active emergency response, prevents misuse.

4.2 Recommendations and Implementation Guidance

1. ANALYZE EMPLOYEE MOVEMENT PATTERNS TO OPTIMIZE SCREENING LOCATIONS

Conduct comprehensive analysis of employee movement patterns using access control data to identify optimal screening locations and justify access point consolidation decisions.

Implementation Guidance: Effective movement pattern analysis requires a multidimensional approach that can include:

- Extracting badge reader transaction data covering all seasons and operational periods to capture full variation
- Analyzing patterns by hour of day, day of week, and seasonal variations to identify peak usage periods and bottlenecks
- Mapping employee pathways through facilities by correlating data from multiple badge readers
- Correlating movement patterns with flight schedules, shift changes, and other operational drivers
- Evaluating the distinction between essential and convenience-based access points
- Using data visualizations to communicate findings to stakeholders and justify consolidation decisions

A data-driven approach provided objective justification for closing underutilized access points and concentrating resources at high-volume locations.

2. INFRASTRUCTURE INTEGRATION WITH CAPITAL PROJECTS

Integrate screening infrastructure development with planned capital improvement projects to minimize costs and operational disruption.

Implementation Guidance: Airports can achieve significant cost savings by incorporating employee screening infrastructure into larger renovation or construction projects. This approach involves:

- Identifying upcoming terminal renovations or expansions early in planning phases
- Establishing separate capital projects for screening equipment while building supporting infrastructure into larger project budgets
- Coordinating with design teams to ensure appropriate space allocation and utility provisions
- Avoiding costly retrofits by planning for screening requirements from project inception

Several airports successfully implemented this strategy, reporting substantial cost savings compared to standalone screening infrastructure projects.

3. IMPLEMENT PHASED DEPLOYMENT APPROACHES

Deploy screening operations incrementally to allow for procedural refinement, stakeholder adaptation, and resource optimization.

Implementation Guidance: Successful phased implementation integrates operational continuity with security enhancement. Key activities can include:

- Starting with pilot programs at single locations to:
 - Test procedures and equipment configurations
 - Train screening personnel in live environments
 - Gather stakeholder feedback for refinement
- Conducting pre-deployment demonstrations by:
 - Setting up actual screening equipment for hands-on stakeholder experiences
 - Inviting employee representatives and union officials to observe operations
 - Addressing concerns before full deployment
- Scheduling incremental checkpoint activation to:
 - Focus resources and training on one location at a time
 - Incorporate lessons learned into subsequent phases

Phased implementation periods ranged from a few days to a few weeks per checkpoint, allowing adequate time for adjustment while maintaining momentum.

4. ESTABLISH FORMAL SCREENING EXEMPTION MANAGEMENT PROCESSES

Develop structured processes for reviewing, granting, and documenting screening exemptions to maintain program integrity while accommodating operational needs.

Implementation Guidance: Effective exemption management requires formal protocols that align security with operational requirements. Key elements can include:

- Establishing clear criteria aligned with:
 - TSA AWS NA populations
 - Locally approved exemptions for critical operations personnel
- Creating management structures including:
 - Formal application processes with operational justification requirements
 - Review boards with security and operations representation
 - Defined approval workflows and authorization levels
- Implementing tracking systems to monitor exempt badge usage patterns and flag anomalies for investigation

Airports with structured exemption management reported better stakeholder acceptance and fewer compliance issues than those using informal processes.

SECTION 4 QUICK REFERENCE

- Analyze access control data to justify consolidation and optimize checkpoint locations
- Design infrastructure with expansion capabilities for full employee screening.
- Integrate screening projects with planned capital improvements
- Establish formal exemption criteria and management protocols

SECTION 5: STAKEHOLDER ENGAGEMENT

Translating the decision to implement full employee screening into an operational program requires coordinated attention to both program design and stakeholder engagement. These two elements are deeply interconnected, as design decisions affect stakeholder acceptance and stakeholder input shapes effective program design.

Effective stakeholder engagement forms the foundation for successful full employee screening program implementation at airports. The complexity of airport operations, combined with diverse workforce populations and multiple organizational entities, demands a structured approach to stakeholder management that builds consensus among competing interests, addresses legitimate concerns about operational impacts, and creates collaborative frameworks that support long-term program sustainability.

This section examines the diverse stakeholder ecosystem that airports must engage when implementing full employee screening programs and explores research findings on how effective engagement practices contribute to program success.

5.1 Building Consensus Through Stakeholder Engagement

The importance of comprehensive stakeholder engagement has been reinforced through research demonstrating that programs developed in isolation often face significant resistance, operational challenges, and compliance issues. By contrast, airports that invest in systematic stakeholder engagement from the earliest planning stages report smoother implementations, improved compliance, and more effective security outcomes. This collaborative approach transforms potential opponents into program advocates while ensuring that operational realities inform program design.

5.1.1 Identifying Stakeholders

The research identified a broad spectrum of stakeholders essential to the success of employee screening programs at airports. Core stakeholders consistently include airport security and operations teams, law enforcement agencies, airlines, tenants and concessionaires, labor unions and employee representatives, regulatory authorities (TSA, CBP, FAA), and third-party service providers. Several airports in our study emphasized that engaging stakeholders who manage daily operations provides critical insights into operational constraints, staffing challenges, and physical layout limitations that might otherwise be overlooked during planning phases.

The research also highlighted the importance of cross-functional stakeholder groups. Several of the interviewed airports established security advisory committees or similar collaborative bodies that bring together airport security directors, TSA FSDs, law enforcement representatives, and key tenant organizations. These diverse teams facilitate enhanced understanding and cooperation, improve information sharing, strengthen compliance efforts, and lead to more effective mitigation strategies against insider threats. Smaller airports with fewer staff can adopt similar outreach and engagement practices on an appropriate scale, tailoring collaborative structures to fit their unique operational environments and resource levels.

5.1.2 Strategic Communication Approaches

Among the airports surveyed, successful stakeholder engagement consistently relied on structured, transparent, and tailored communication strategies. Most airports emphasized that effective communication must address specific stakeholder concerns while maintaining consistent core messaging

about security objectives. Communication channels utilized by the airports we spoke with include scheduled meetings and briefings, tailored publications for different workforce segments, digital platforms (including QR codes and social media), formal communication embedded within ID media applications, and integration with SIDA training programs.

Several airports in our study implementing full employee screening utilized extensive informational campaigns incorporating multiple communication mediums. These campaigns typically featured strategic placement of signage and posters, dedicated digital communication platforms, targeted briefings for specific workforce populations, and regular updates through established airport communication channels. The research found that multichannel approaches significantly improved message penetration and stakeholder understanding.

5.1.3 Employee Communication and Education

Airports in this study emphasized the importance of educating employees about screening procedures and their rights. Multiple airports attributed success in avoiding legal challenges to thorough communication plans that clearly established legal authority for screening and provided transparent information about the process. Effective employee communication strategies include using multiple channels such as direct email notifications to authorized signatories, working through industry associations to reach airlines, and deploying employee mobile applications that send real-time notifications. Direct interaction through in-person meetings or phone calls was reported as more impactful than relying only on bulletins or email messages. The combination of in-person, verbal, and written communication is most effective, although more time-consuming.

Some airports developed video demonstrations showing how to use new screening technology, distributed through airport employee apps. One airport highlighted the importance of explaining the “why” behind screening requirements, focusing not only on the fact that TSA mandated it but also on the specific security reasons motivating implementation. Education programs typically address screening procedures and expectations, employee rights during screening, accommodation request processes, complaint and feedback mechanisms, and privacy protections in place. Airports found that comprehensive education reduced resistance, minimized legal challenges, and improved overall program acceptance.

5.1.4 Addressing Stakeholder Concerns

The airports interviewed repeatedly stressed that proactively addressing stakeholder concerns prevents minor issues from escalating into major obstacles. Key areas of concern identified through the research include privacy implications of screening procedures, potential impacts on shift timing and workforce scheduling, perceived fairness and consistency of screening practices, and operational disruptions during peak periods.

Many airports in the research found that engaging employee representatives and labor unions early in the planning process helped address workforce concerns before they became entrenched positions. Successful approaches included structured negotiation processes, incorporation of stakeholder feedback into program design, transparent communication about security objectives and constraints, and development of procedures that integrate security requirements with operational needs.

5.1.5 Facilitating Collaborative Program Development

Research findings indicate that joint training or demonstration sessions involving multiple stakeholders significantly enhance program effectiveness. These collaborative activities serve multiple purposes: identifying potential procedural gaps before implementation, building mutual understanding among diverse stakeholder groups, creating opportunities for creative problem-solving, and establishing relationships that facilitate ongoing coordination.

Several airports in our study implemented pilot programs or phased implementations that allowed stakeholders to experience procedures firsthand before full deployment. This approach provided valuable opportunities to refine procedures based on real-world feedback, build stakeholder confidence through demonstrated success, identify and address unexpected operational impacts, and develop solutions collaboratively with affected parties.

5.1.6 Developing Continuous Engagement Mechanisms

Stakeholder engagement extends well beyond initial implementation, requiring sustained effort to maintain program effectiveness. Most airports surveyed established formalized forums or committees for ongoing stakeholder coordination. Common structures include airport security consortia bringing together all security stakeholders, regular working group meetings focused on specific operational areas, feedback mechanisms including surveys and anonymous reporting options, and structured review processes for procedure updates.

The research identified several critical success factors for ongoing engagement. Most airports in the research emphasized the importance of:

- Visible senior executive support demonstrating the airport's commitment to full employee screening
- Regular communication maintaining stakeholder awareness and buy-in
- Responsive feedback systems showing that stakeholder input is valued
- Adaptive management approaches that allow programs to evolve based on operational experience

5.2 Recommendations and Implementation Guidance

1. CREATE A COMPREHENSIVE COMMUNICATION FRAMEWORK

Implement a structured communication plan utilizing multiple channels appropriate to different stakeholder groups and program phases.

Implementation Guidance: Effective communication requires reaching diverse audiences:

- Create written materials that clearly explain the legal authority for screening, outline what to expect during the screening process, detail prohibited items policies, and describe accommodation request procedures
- Establish regular communication cadences (e.g., weekly or monthly) during planning, implementation, steady-state operations, and significant changes
- Leverage multiple communication channels such as:
 - Digital platforms and email updates
 - Printed materials for common areas
 - Dedicated information session

- Conduct training sessions for all badge holders prior to program implementation
- Establish feedback mechanisms so employees can raise concerns or suggest improvements while maintaining program integrity
- Regularly update communication materials to reflect operational changes, lessons learned, and employee feedback

2. IMPLEMENT EARLY ENGAGEMENT PROTOCOLS

Initiate stakeholder engagement during the earliest planning stages to incorporate operational insights and build consensus.

Implementation Guidance: Early engagement helps identify and address concerns proactively:

- Convene stakeholder forums well before implementation to gather input on operational constraints and workforce impacts
- Establish feedback mechanisms so employees can raise concerns or suggest improvements while maintaining program integrity
- Larger airports may benefit from establishing topic-specific working groups for complex issues
- Regularly update communication materials to reflect operational changes, lessons learned, and employee feedback

3. DEVELOP COLLABORATIVE PROBLEM-SOLVING MECHANISMS

Establish processes for stakeholders to collaboratively address challenges and develop solutions.

Implementation Guidance: Create opportunities for joint problem-solving:

- Form cross-functional teams with representation from major stakeholder groups
- Schedule regular working sessions to address operational challenges
- Use pilot programs, demonstrations, or tabletop exercises to evaluate procedures, refine processes, and gather feedback

4. ESTABLISH FORMAL COORDINATION STAKEHOLDER STRUCTURES

Create governance structures that integrate stakeholder engagement throughout the program life cycle.

Implementation Guidance: Formal structures ensure sustained coordination:

- Develop an airport security working group or similar body with:
 - Defined membership representing key stakeholders
 - Regular meeting schedule (e.g., quarterly)
 - Clear communication protocols
- Use existing airport committees where possible to avoid duplication

5. LEVERAGE EXECUTIVE CHAMPIONSHIP

Secure visible senior executive support from airport leadership and key stakeholder organizations.

Implementation Guidance: Executive support drives stakeholder participation:

- Engage senior leaders to communicate and reinforce program importance and benefit (or rationale) to the community
- Have executives participate in key stakeholder meetings and employee forums
- Leverage executive influence to address concerns and maintain momentum

SECTION 5 QUICK REFERENCE

- Identify and engage all key stakeholders early in the planning process
- Implement multichannel communication strategies tailored to different groups
- Address concerns proactively through collaborative problem-solving
- Establish formal coordination structures for sustained engagement, evolution, and continuous improvement
- Secure visible executive support to drive participation

SECTION 6: SCREENING INFRASTRUCTURE

Infrastructure decisions form the physical foundation of full employee screening programs. Once implemented, infrastructure investments can be difficult and costly to modify, making thorough planning essential before committing resources.

6.1 Strategic Infrastructure Planning and Checkpoint Design

Effective screening infrastructure planning forms the cornerstone of any successful full employee screening program, requiring airports to integrate security imperatives with operational efficiency while working within physical and financial constraints. The strategic placement and design of screening checkpoints directly impact program effectiveness, employee compliance, operational flow, and resource requirements. The complexity of modern airport facilities, combined with the need to screen employees across multiple shifts and operational periods, demands a systematic approach to infrastructure development. Without thoughtful infrastructure planning, even well-funded programs can fail due to bottlenecks, excessive wait times, or inadequate coverage of critical access points.

For airports with capital project opportunities, design-phase integration should be the first consideration, as terminal design decisions will shape all subsequent infrastructure possibilities. Airports working within existing facilities will also find guidance on retrofit scenarios in the subsections that follow.

6.1.1 Leveraging Capital Projects for Screening Infrastructure

For airports with planned, in-progress, or anticipated terminal construction or major renovation projects, the design phase is the optimal time to address full employee screening infrastructure. This applies whether an airport is committed to implementation or simply preserving flexibility for future consideration. Design choices made during capital projects will determine available space for screening checkpoints, infrastructure capacity, access point configurations, and construction approaches. For this reason, airports with capital project opportunities should address design-phase integration before other infrastructure planning considerations.

COST AND COMPLEXITY ADVANTAGES OF DESIGN-PHASE INTEGRATION

Incorporating full employee screening requirements into capital projects avoids the higher costs and complexity associated with retrofitting existing facilities. Six airports in the study incorporated or planned to incorporate screening infrastructure into new terminal construction or renovation projects. These airports reported that integrating screening requirements during construction allowed them to ensure sufficient space, data connectivity, power supply, and other infrastructure were available when programs were implemented. One airport noted that incorporating screening requirements into early design phases added minimal cost compared to post-construction modifications, while another identified infrastructure as the primary cost consideration beyond staffing contracts.

EARLY DESIGN INTEGRATION

Three airports incorporated screening requirements into architectural plans and design specifications before construction began. This approach allowed screening infrastructure to be embedded into terminal layouts rather than added as modifications to completed designs. One airport incorporated screening locations into terminal renovation plans to be proactive ahead of potential future requirements. Another airport planned access points during the initial design phase of a new terminal, while a third leveraged a terminal lobby expansion to integrate screening into the design.

Additionally, two airports communicated potential future screening requirements to project managers and design teams even when full employee screening had not yet been formally approved. This approach preserved flexibility to incorporate screening infrastructure if later decided upon, without committing to full implementation during the design phase.

DESIGN CONSIDERATIONS FOR SCREENING-OPTIMIZED FACILITIES

Airports undertaking capital projects have opportunities to design facilities that optimize full employee screening operations. Key design considerations identified in the research include:

- **Access Point Consolidation:** Terminal designs can reduce the number of employee access points, concentrating screening at fewer locations to improve efficiency and reduce staffing requirements. Terminal redesign projects create opportunities to reduce access points, a key strategy for improving screening efficiency.
- **Space Allocation:** Architectural designs can allocate sufficient space for screening checkpoints, queuing areas, and alarm resolution. Airports that planned space during design phases avoided the constraints that limit checkpoint options in existing facilities.
- **Utility Provisioning:** Construction projects provide opportunities to ensure adequate electrical capacity, data connectivity, and HVAC infrastructure to support screening technologies. Electrical capacity and data connectivity emerged as important considerations, with various airports noting that existing infrastructure required costly upgrades to support screening equipment.
- **Scalability:** Designing infrastructure with future expansion in mind allows airports to add screening lanes, incorporate new technologies, or expand capacity as employee populations or requirements change.

FLEXIBILITY THROUGH CONTRACT STRUCTURE

The use of design-build contracts has proven effective among some airports for maintaining flexibility during construction and implementation phases. This contract structure allows for adjustments based on operational feedback and evolving requirements.

STAKEHOLDER COORDINATION DURING DESIGN PHASE

Successful integration of full employee screening into capital projects requires early coordination with multiple stakeholders:

- Capital planning and project management teams to identify suitable projects and align timelines
- Design architects to incorporate screening space into terminal layouts
- Engineering teams to ensure adequate utilities (electrical, HVAC, data)
- Construction managers to phase screening infrastructure appropriately
- TSA FSDs to align with regulatory requirements

Early engagement with these stakeholders during design phases helps ensure that screening requirements are incorporated before designs are finalized and changes become costly.

6.1.2 Airports Without Near-Term Capital Projects

For airports working within existing facilities without planned construction or renovation projects, this section provides guidance on infrastructure planning for retrofit scenarios, including analyzing employee movement patterns, optimizing checkpoint placement within existing constraints, evaluating remote screening alternatives, and assessing space and infrastructure requirements.

NUMBER AND LOCATION OF SCREENING ACCESS POINTS

Determining the optimal number and placement of screening access points is critical to program effectiveness and operational efficiency. Airports must align security coverage with practical constraints including physical space, employee flow patterns, stakeholder impacts, and resource availability. Many of the research airports employed data-driven approaches to inform these decisions, analyzing employee movement patterns and coordinating closely with stakeholders to identify locations that maximize security while minimizing operational disruption.

EMPLOYEE MOVEMENT PATTERN ANALYSIS

Historical data from access control systems enables analysis of employee movement patterns across multiple dimensions and informs screening point placement decisions. Among the airports interviewed, this analysis typically examines badge reader transactions across multiple dimensions including time of day, day of week, and seasonal variations. This method helps airports justify the strategic closure or restriction of less-utilized entry points, enhancing both security and operational efficiency.

Comprehensive movement pattern analysis revealed surprising patterns, such as significant volumes during traditionally off-peak hours due to shift changes, maintenance activities, or cargo operations. Additionally, airports acknowledge the complexity introduced by high-traffic areas, emphasizing the importance of comprehensive flow analysis to avoid operational bottlenecks and maintain smooth employee throughput during peak periods.

OPTIMAL CHECKPOINT PLACEMENT

Optimal checkpoint placement requires extensive collaboration with stakeholders such as airlines, tenants, real estate representatives, and regulatory agencies. Airports have underscored the importance of this coordination to effectively manage operational disruptions and ensure buy-in for checkpoint locations.

Physical infrastructure and space constraints also play a central role in determining checkpoint placement. Several airports in our research carefully estimated the required number of access points necessary to support comprehensive screening programs. Leveraging terminal expansions can simplify checkpoint infrastructure requirements and create centralized, efficient screening locations.

Additionally, airports have recognized the challenge presented by legacy infrastructure, such as older terminals with fragmented layouts and multiple checkpoints, which complicate centralized screening. Incorporating checkpoint planning into new terminal designs or major renovation projects allows airports to proactively address insider threats and anticipated regulatory changes, reducing the need for costly retrofitting.

6.1.3 Remote Screening Locations

For airports facing terminal space constraints that preclude conventional checkpoint placement, remote screening locations offer an alternative approach. Several airports have successfully implemented full employee screening at remote parking facilities to address space constraints and operational efficiency challenges. This innovative approach involves establishing screening checkpoints at employee parking lots located away from terminal buildings. This model typically includes:

- Dedicated screening facilities at remote employee parking areas
- Creation of a “rolling Sterile Area” where employees are screened before boarding buses
- Secure transportation systems maintaining the sterile environment during transit to terminals
- Contingency procedures for vehicle breakdowns requiring rescreening

One airport implemented this approach using four screening buildings at their off-site employee parking lot within the AOA, with dedicated buses transporting pre-screened employees to various concourses. Another airport established checkpoints at employee parking adjacent to the AOA fence, with bus pickups inside the secure area.

While this approach requires initial infrastructure investment for shelters, equipment, and power systems, it offers several advantages: convenient screening at the point where employees naturally congregate, reduced congestion at terminal access points, and efficient use of existing parking facilities. This solution has proven particularly valuable for airports facing terminal space constraints or seeking to minimize operational disruptions during terminal renovations.

6.1.4 Contingency Access Planning

Planning for contingency access points ensures operational continuity during emergencies, technology failures, or significant maintenance events. Airports emphasized emergency response coordination as a critical component of contingency planning, regularly engaging local fire inspectors, building officials, and emergency response personnel during design and implementation to align with fire safety and building codes. Operational flexibility is also paramount, and several airports adopted measures to ensure adaptability to unforeseen disruptions, including infrastructure or technology failures.

6.1.5 Space and Infrastructure Needs

Successful implementation of full employee screening programs requires careful assessment of physical space availability and supporting infrastructure capabilities. Space constraints and infrastructure requirements were consistently identified as critical factors influencing program design, with facility limitations often determining feasibility, technology selection, and operational approaches. For airports working within existing facilities, this assessment focuses on evaluating current conditions and identifying necessary modifications, whereas airports with capital projects can address these requirements through design-phase planning.

PHYSICAL SPACE REQUIREMENTS

Space and infrastructure considerations play a crucial role in the feasibility and effectiveness of full employee screening programs, with airports consistently identifying space constraints as a major implementation challenge. Among the airports surveyed, space requirements vary significantly based on employee volumes, screening technology choices, and operational models. Several airports interviewed highlighted space availability as a primary deciding factor influencing their decision-making.

INFRASTRUCTURE AND UTILITY REQUIREMENTS

Full employee screening programs require careful planning of utilities and service infrastructure. Airports reported the necessity of enhancements to electrical systems, IT networks, telecommunications, and HVAC systems to accommodate screening technologies. Electrical capacity and data connectivity emerged as crucial considerations, requiring coordination with engineering and IT departments early in the design stage to ensure infrastructure compatibility. Several airports noted challenges associated with existing infrastructure that did not initially support modern security technologies, requiring retrofits and additional upgrades, including high-speed network connections, to ensure seamless operation of new screening technologies.

Airports retrofitting screening into older terminals also encountered structural limitations and regulatory compliance considerations, including adherence to local building codes and ADA requirements. Coordination with local fire marshals, engineering departments, and regulatory bodies is particularly

important when modifying existing facilities, especially regarding emergency egress pathways and compliance with local building and safety codes.

Camera systems represent essential security infrastructure that must be integrated into checkpoint design from the planning phase. Coverage requirements should include comprehensive views of all screening positions, queue areas, and divestiture locations to support both real-time monitoring and incident review. Physical infrastructure for camera systems requires consideration of mounting locations, power requirements, network connectivity for digital systems, and secure storage capacity for retention of recorded footage according to regulatory and operational requirements.

6.2 Recommendations and Implementation Guidance

1. INTEGRATE SCREENING REQUIREMENTS INTO CAPITAL PROJECTS AND NEW CONSTRUCTION

Incorporate full employee screening requirements into terminal renovation, expansion, or new construction projects to optimize checkpoint placement, avoid costly retrofits, and ensure infrastructure supports current and future screening needs.

Implementation Guidance: Airports achieved cost efficiencies and better infrastructure outcomes by incorporating screening requirements into capital projects. Implementation approaches vary based on project stage and commitment level:

For airports in early design phases of new construction or major renovation:

- Engage security, operations, and capital planning teams during earliest design phases to ensure screening requirements are considered alongside other project priorities
- Work with architects and engineers to embed screening infrastructure into terminal layouts, including space for checkpoints, queuing areas, and alarm resolution
- Design terminal configurations that reduce or consolidate employee access points, facilitating more efficient screening operations
- Ensure utility provisioning (electrical capacity, data connectivity, HVAC) supports current or planned screening technologies
- Consider designing infrastructure with scalability in mind, allowing for potential addition of screening lanes or expanded capacity as requirements evolve
- Consider design-build contract structures to maintain flexibility for screening technology updates during construction phases

For airports with projects in later design stages or already under construction: While opportunities to influence fundamental design decisions may be limited, airports can still coordinate with project teams to identify remaining integration opportunities. Consider establishing separate capital projects for screening equipment while ensuring supporting infrastructure (electrical, data, HVAC) is incorporated into the main construction budget before the project is completed.

For airports not yet committed to full employee screening:

- Communicate potential future screening requirements to project managers and design teams during capital planning processes
- Evaluate whether including basic infrastructure provisions (space allocation, power capacity, data connectivity) would preserve flexibility for future security enhancements without significant additional cost

For business case considerations regarding infrastructure costs and strategic timing decisions, see Section 2.1.

2. ANALYZE EMPLOYEE MOVEMENT PATTERNS TO OPTIMIZE SCREENING LOCATIONS

Conduct comprehensive analysis of employee movement patterns using access control data to identify optimal screening locations and resource allocation strategies.

Implementation Guidance: Airports may extract badge reader transaction data covering all operational periods and seasons to understand movement patterns. Key implementation steps observed include:

- Analyzing access point usage by hour, day of week, and season to identify patterns
- Evaluating employee volumes during peak and off-peak periods to anticipate potential bottlenecks
- Mapping primary employee pathways through terminal facilities
- Correlating movement patterns with flight schedules, shift changes, and cargo operations
- Some airports have found success using this data to justify consolidating underutilized access points and concentrating resources at high-volume locations

3. OPTIMIZE SCREENING CHECKPOINT PLACEMENT

Select employee screening checkpoint locations through systematic evaluation of operational impacts, physical constraints, and stakeholder requirements.

Implementation Guidance: Checkpoint placement decisions may balance security requirements with operational efficiency. Airports emphasized several key considerations:

- Assessing physical space availability and infrastructure constraints at potential locations
- Evaluating terminal-specific factors, including the number of portals required based on layout and employee volumes
- Coordinating with airlines, tenants, and regulatory agencies to manage operational impacts
- Integrating checkpoint requirements into existing or planned terminal configurations
- Ensuring compliance with life-safety requirements in local building codes and ADA regulations
- Some airports have found opportunities to incorporate checkpoint planning into major renovation projects, reducing future retrofit costs

4. ESTABLISH CONTINGENCY ACCESS PROCEDURES

Develop alternative access protocols to maintain operational continuity during emergencies, technology failures, or significant maintenance events.

Implementation Guidance: Effective contingency planning typically requires coordination with multiple stakeholders and regular testing of backup procedures. Key implementation approaches observed include:

- Coordinating with local fire inspectors, building officials, and emergency response personnel during design phases
- Developing alternative screening procedures for technology failures or equipment maintenance
- Training security staff on manual screening protocols and emergency bypass procedures
- Maintaining designated emergency access points with enhanced manual screening capabilities
- Conducting regular tabletop exercises to test contingency procedures with stakeholders

SECTION 6 QUICK REFERENCE

- Conduct comprehensive movement pattern analysis using access control data and observations
- Develop strategic infrastructure plans that balance current needs with future flexibility
- Optimize checkpoint placement through systematic evaluation of operational factors
- Establish contingency procedures for operational continuity during disruptions
- Integrate screening infrastructure with planned capital projects when feasible
- Engage stakeholders early and maintain ongoing coordination throughout planning
- Consider design-build contracts for implementation flexibility
- Plan for adequate power, network, and utility infrastructure from project inception

SECTION 7: SCREENING TECHNOLOGY

Technology investments are a core component of full employee screening programs, influencing detection capabilities, processing efficiency, and long-term operational costs alongside factors such as screening procedures, personnel, and training. Unlike infrastructure decisions that are largely fixed once implemented, technology choices offer ongoing opportunities for enhancement but also require sustained attention to life cycle management, vendor relationships, and evolving capabilities.

7.1 Technology Selection and Investment Decisions

This section examines how airports approach technology selection decisions, including evaluation frameworks, acquisition strategies, cost management practices, and life cycle planning considerations. The selection and implementation of appropriate screening technologies represent a fundamental investment decision that significantly impacts both the effectiveness and efficiency of full employee screening programs. Technology choices directly influence detection capabilities, throughput rates, staffing requirements, and long-term operational costs. Airports must navigate a complex landscape of available technologies while balancing security effectiveness with operational practicality, budget constraints, and employee acceptance.

Cost management considerations permeate every aspect of technology decision-making, from initial acquisition through end-of-life disposal. Successful programs recognize that the lowest purchase price rarely represents the best value, and that strategic investments in redundancy, maintenance agreements, and quality equipment often yield lower total costs over the equipment life cycle.

Beyond initial acquisition decisions, successful technology implementation requires comprehensive planning for life cycle management, maintenance requirements, and future technology considerations. The evolution of screening technologies, combined with changing threat landscapes and regulatory requirements, demands strategic approaches to technology selection that consider not only current needs but also future scalability and integration capabilities. While these technology investments may not represent the largest capital expenditure compared to major airport infrastructure projects, they can be significant investments particularly for smaller to mid-sized airports, requiring careful evaluation and planning before committing resources.

7.1.1 Technology Options and Capabilities

Research participants utilize a wide array of screening technologies ranging from badge readers and simple metal detectors to sophisticated advanced imaging systems and multilayered surveillance systems. Technology selection varied significantly based on airport size, threat assessment, and available resources.

Table 3 summarizes the screening technologies currently deployed or planned for implementation among the 26 US airports in this study, categorized by airport classification. The data reveals significant variation in technology adoption across airport categories, with Category X airports implementing more advanced and integrated technologies while smaller airports relied primarily on handheld metal detectors and manual screening processes.

Table 3. Screening Technology Implementation by Airport Category

Technology Category	Airports Currently Using by Category	Airports Planning to Implement by Category
ON-PERSON SCREENING		
AIT / Body Scanners	5 total • CAT X: 5	2 total • CAT X: 1 • CAT I: 1
WTMD	16 total • CAT X: 12 • CAT I: 4	—
Handheld Metal Detector	24 total • CAT X: 15 • CAT I: 7 • CAT II: 2	—
ACCESSIBLE PROPERTY SCREENING		
X-ray Equipment	14 total • CAT X: 11 • CAT I: 2 • CAT II: 1	—
AI-Enhanced Detection Algorithms	2 total • CAT X: 2	—
ETD systems	7 total • CAT X: 6 • CAT I: 1	16 total • CAT X: 11 • CAT I: 3 • CAT II: 2
ACCESS CONTROL		
Biometric Authentication	2 total • CAT X: 2	—
E-Gates	1 total • CAT X: 1	—
Mobile Card Readers	1 total • CAT X: 1	—

While many airports have implemented biometric technology with access control systems, only two airports specifically reported integrating biometric technology in connection with their full employee screening programs. One airport reported using a biometric reader that scans both the employee's badge and fingerprint before the screening checkpoint. The other airport integrated facial recognition with an e-gate system at the entrance of its screening portals and reported reduced staffing needs due to the automated identity verification capability.

AIT adoption has enabled screening for metallic and non-metallic threats and other contraband concealed on a person before entering airport secured areas. Some AIT systems enable aviation workers to pass through screening without having to remove personal items, streamlining the screening process and improving throughput. Multiple airports in our study reported implementing body scanner systems,

with one airport specifically noting they worked with the vendor to tune and refine algorithms for their specific requirements, focusing on guns, knives, and explosives in priority order. Another airport reported conducting 1,400–1,500 scans across various body types and genders to provide data for algorithm development.

Artificial intelligence and automated threat detection emerged as a noteworthy trend among research airports. Three screening operations in our research have implemented AI-enhanced x-ray systems with automatic threat detection capabilities. One airport reported that its AI threat detection software outperforms humans in both accuracy and speed, operating continuously and automatically stopping the belt when alarms occur. Another reported that prohibited item detection software provides better detection accuracy and reliability than human operators, describing it as “consistently better than human operators,” while acknowledging it is not 100% perfect.

7.1.2 Technology Investment Decision Criteria

When evaluating screening technology investments, airports and airlines operating their own screening programs must balance multiple factors beyond initial purchase price. One research participant reported using three primary criteria to guide security technology investment decisions:

1. Enhancement of threat mitigation value
2. Improvement of throughput efficiency
3. Improvement of customer experience for employees

This framework helps organizations evaluate whether advanced technologies justify their costs when scaled across multiple locations. For example, while advanced body scanners that detect non-metallic objects provide superior threat detection compared to WTMDs, the cost differential becomes substantial when multiplied across a dozen or more checkpoints. Airports should consider developing similar evaluation frameworks that align technology investments with their specific security objectives, operational requirements, and financial constraints.

7.1.3 Acquisition Strategies

Airports employ diverse acquisition strategies for screening technology, with approaches varying based on budget availability, procurement regulations, and operational requirements. Most airports surveyed utilize formal procurement processes including Request for Information (RFI), Request for Proposal (RFP), and Request for Quotation (RFQ) to ensure competition, transparency, and alignment with airport requirements.

Acquisition decisions should compare upfront purchase price with long-term operational and maintenance costs through comprehensive life cycle cost analysis. Capital expenditures for screening technology infrastructure vary significantly based on airport size and program scope. For example, one airport invested approximately \$5.6 million in dedicated employee screening checkpoints and vehicle checkpoints at perimeters, while another exceeded \$25 million for nine new screening portals with advanced technology. Beyond capital costs, ongoing expenses including training, staffing, maintenance, and utilities are essential factors in selecting the appropriate procurement approach.

Two airports in our research reported that they leveraged construction or design-build contracts to include equipment purchases, shortening procurement timelines. One airport specifically used a design-build contract with a primary contractor to manage technology integration, requiring vendors to support the integration of supporting capabilities, such as third-party threat detection algorithms.

Integrated procurement approaches can also simplify contract management while supporting cost sustainability, particularly for smaller or mid-sized airports with limited budgets. One airport described plans to award a security service contract that included acquisition, deployment, installation, and maintenance of security equipment, combining personnel services, equipment procurement, and equipment maintenance under a single contract. The airport representative noted that managing, “one contract that does all three of those versus three separate contracts in our procurement process is a much simpler thing for me and much more attractive.” This strategy allows airports to specify performance requirements rather than specific equipment models, enabling vendors to propose solutions that best meet operational needs while leveraging their expertise about available technologies.

7.1.4 Leveraging Cooperative Purchasing Programs

Airports can significantly streamline security equipment procurement by utilizing the General Services Administration (GSA) Cooperative Purchasing Program, which provides state, local, and tribal government entities—including public airport authorities—access to security screening equipment through GSA Advantage and GSA Multiple Award Schedule contracts.⁴⁴ Under this program, eligible airports can purchase security equipment from GSA Schedule contractors who have opted into cooperative purchasing, accessing pre-negotiated government pricing and terms. The GSA Cooperative Purchasing Program offers access to security screening equipment under Large Category J (Security & Protection), particularly through SIN 334519 (Bomb & Hazardous Material Disposal; Metal & Bomb Detection), which includes WTMD, hand-held metal detector, ETD, x-ray, and other explosive detection equipment from a range of manufacturers.

Public airport authorities qualify as eligible non-Federal entities under GSAM 538.7001, which defines eligible entities to include any state or local government “or any instrumentality thereof.” This classification allows airports to purchase security equipment supporting homeland security missions directly through GSA Advantage using purchase cards or through GSA eBuy for competitive quotes among schedule holders. Airports must follow their own procurement rules while leveraging GSA’s pre-competed contracts, potentially reducing procurement timelines and administrative burden.

Additionally, airports may explore the DoD 1122 Program (10 U.S.C. §381), which allows states and local governments to purchase qualifying equipment through DoD-coordinated sources for homeland security and emergency response missions.⁴⁵ Security screening equipment typically qualifies under the homeland security mission, though purchases must be equipment-only and coordinated through a designated State Point of Contact. When using the 1122 Program, airports must include GSA’s mandatory order language and obtain State Point of Contact approval before purchase.

Other cooperative purchasing options that airports may consider include programs like OMNIA Partners and Sourcewell, though additional research would be needed to confirm the availability of security screening equipment through these specific programs. These cooperative purchasing vehicles can reduce the administrative burden of conducting independent solicitations, which can be particularly beneficial for smaller airports with limited procurement resources.

⁴⁴ “GSA Cooperative Purchasing Program,” *U.S. General Services Administration*, accessed October 15, 2025, <https://www.gsa.gov/buy-through-us/purchasing-programs/programs-for-state-and-local-government/cooperative-purchasing-program>.

⁴⁵ 10 U.S.C. § 381 (“DoD 1122 Program”); “Learn about the 1122 program,” *U.S. General Services Administration*, accessed October 15, 2025, <https://www.gsa.gov/buy-through-us/purchasing-programs/programs-for-state-and-local-government/1122-program>.

7.1.5 Security Equipment Cost Management

Research participants shared a range of strategies for managing equipment procurement and maintenance expenses. Several emphasized the importance of planning for equipment redundancy, with one airport noting their new checkpoint has dual lanes not primarily for capacity but for redundancy, ensuring that screening can continue if one x-ray machine is out of service. This approach, while requiring higher initial investment, prevents costly operational disruptions and overtime expenses when equipment failures occur and personnel are forced to revert to manual search procedures.

Establishing detailed SLAs with equipment manufacturers was stressed by three airports as essential for cost control. One international airport described requiring specific maintenance response times, local storage of spare parts, and penalty clauses for non-compliance in their maintenance contracts. These agreements help airports avoid unexpected repair costs and minimize expensive downtime. Another airport learned this lesson the hard way, having to request millions in additional funding from their board when manufacturer warranties expired because service agreements were not included in the original procurement.

Regular preventive maintenance was consistently cited as a cost-saving measure that extends equipment life and reduces both downtime and emergency repair expenses. Multiple airports emphasized evaluating not just initial purchase price but total cost of ownership when selecting equipment. As one airport noted, a system based on low-cost equipment could prove more expensive over the operational life due to higher maintenance and replacement costs. This total cost perspective helps airports make more informed decisions that optimize long-term value rather than minimizing short-term expenditure.

7.1.6 Technology Life Cycle Management

Effective life cycle management of screening technology is essential for maintaining reliability, minimizing downtime, and ensuring continued operational effectiveness. These practices directly impact long-term costs, as proper maintenance can extend equipment life by years and reduce the frequency of expensive emergency repairs. Airports interviewed consistently emphasized the importance of preventive maintenance schedules, multi-year service agreements, and proactive calibration practices to maintain equipment performance.

Regular calibration emerged as particularly important for ETD equipment among the airports surveyed. Multiple airports reported challenges with ETD reliability, with one airport noting their ETD units are “out of service frequently,” and recommended purchasing additional units for redundancy—specifically, they ordered eleven units when only seven were operationally required. Environmental factors also impact ETD performance, with one airport reporting that 95% humidity caused ETD false alarms, requiring specialized calibration procedures. A number of airports highlighted specific maintenance practices including maintaining spare parts inventories and establishing vendor support agreements. One airport purchased more ETD units than operationally required (nine instead of three) to allow for hot-swapping and equipment maintenance downtime.

Among the airports surveyed, best practices for life cycle management included maintaining spare parts inventories, establishing vendor support agreements, and implementing structured maintenance tracking systems. Multiple airports emphasized oversight of SLAs, with one airport noting they had to return to their board for additional funding when manufacturer warranties expired because service agreements were not included in original procurement. Documentation of maintenance activities was also highlighted for identifying trends, predicting failures, and justifying technology refresh investments.

7.1.7 Technology Refresh Planning

Early planning of refresh cycles was frequently highlighted, with airports noting that proactive planning enables effective cost management and ensures long-term security effectiveness. Staying current with emerging technological trends and regularly evaluating technology performance supports long-term program effectiveness.

Replacement cycles are established in alignment with budget planning processes and technological obsolescence timelines. Multiple airports emphasized avoiding vendor lock-in situations and ensuring flexibility for future upgrades when selecting screening technologies.

7.2 Recommendations and Implementation Guidance

1. DEVELOP STRATEGIC TECHNOLOGY EVALUATION FRAMEWORKS

Establish structured evaluation criteria for evaluating technology investments across multiple dimensions to support informed decision-making.

Implementation Guidance: Airports should consider developing evaluation frameworks tailored to their specific security objectives, operational requirements, and financial constraints. One effective approach evaluates each technology by:

- Assessing whether the technology enhances threat mitigation value by improving detection capabilities for priority threats
- Assessing how the technology impacts screening throughput, staffing requirements, and overall operational efficiency to ensure effective processing during both regular and peak periods
- Factoring how the technology affects the daily screening experience for employees, ensuring that selections support both security and staff satisfaction

2. CONDUCT COMPREHENSIVE TECHNOLOGY ASSESSMENTS

Perform systematic evaluations of screening technologies through pilot testing, operational validation, and life cycle cost analysis before committing to full-scale acquisition decisions.

Implementation Guidance: Several effective approaches to technology assessment have been identified:

- Implement pilot programs prior to full deployment to identify and address training, procedural, technical, and human factors challenges, ensuring smoother and more effective scaling of full employee screening checkpoints.
- Test technology in real-world operating environments to identify and address potential environmental or technical challenges before full deployment.
- Consider the importance of selecting technologies that perform effectively in both indoor and outdoor settings, ensuring reliable operation regardless of installation location and mitigating risks associated with environmental variability.
- Conduct total cost of ownership analyses that account for all expenses over the technology's life cycle, including installation, training, maintenance, spare parts, and disposal, rather than focusing solely on purchase price.
- Assess the vendor's support capabilities and responsiveness, as reliable vendor assistance and stability are essential for successful technology implementation.

3. IMPLEMENT STRATEGIC ACQUISITION APPROACHES

Develop procurement strategies that leverage available contracting mechanisms while ensuring competitive selection and long-term value optimization.

Implementation Guidance: Research participants employed various successful acquisition strategies:

- Choose procurement vehicles that fit the airport's jurisdiction, such as traditional RFI/RFP/RFQ processes or alternative methods to streamline acquisition.
- Investigate cooperative purchasing programs, including GSA Schedule contracts and the DoD 1122 Program, to access pre-negotiated pricing and terms for security screening equipment.
- Consider integrated service contracts that combine equipment, deployment, installation, and maintenance in a single agreement to simplify contract management.
- Include multiyear service agreements, training, and spare parts in initial acquisitions to reduce operational disruptions and unexpected expenses.
- Structure contracts to allow flexibility for system integration and future technology upgrades, avoiding vendor lock-in.

4. ESTABLISH COMPREHENSIVE LIFE CYCLE AND COST MANAGEMENT PROGRAMS

Develop maintenance and support programs that maximize equipment reliability and minimize operational disruptions while optimizing total cost of ownership throughout the technology life cycle.

Implementation Guidance: Participating airports identified critical practices for managing both operational and financial aspects of screening technology:

- Analyze total cost of ownership by factoring in purchase, installation, training, maintenance, consumables, staffing requirements, and disposal costs; higher upfront investments in reliable equipment often reduce long-term expenses.
- Incorporate strategic redundancy into critical systems to minimize operational disruptions and ensure continuous functionality.
- Implement documentation systems to track required maintenance, system performance, failures, and costs, which can help predict issues, support funding justifications, and identify cost-saving opportunities.

5. PLAN FOR TECHNOLOGY EVOLUTION AND REFRESH CYCLES

Establish proactive technology planning processes that anticipate obsolescence and enable timely upgrades aligned with security requirements and budget cycles.

Implementation Guidance: Emphasize the importance of forward-looking technology planning:

- Coordinate technology refresh planning with capital budget cycles, typically scheduling major upgrades 5 to 7 years in advance to align with funding availability.
- Stay informed about emerging technology trends and industry best practices by regularly monitoring developments and engaging with peer organizations.
- Develop clear procedures for equipment disposal and system transition, including documented steps for decommissioning and secure data handling to ensure compliance with environmental regulations.

6. OPTIMIZE TECHNOLOGY INTEGRATION AND OPERATIONS

Deploy integrated screening systems that maximize throughput efficiency while maintaining security effectiveness through strategic use of automation and process optimization.

Implementation Guidance: Airports in the research with more technologically advanced screening operations demonstrated several best practices for technology integration:

- Consider integrating AI and automated detection systems to strengthen security effectiveness and improve operational efficiency.
- Consider combining complementary technologies, such as biometric authentication, remote screening and networked monitoring, to streamline operations and reduce staffing needs.
- Consider utilizing advanced technology solutions to address challenges related to staffing or training limitations and support more consistent screener performance.

SECTION 7 QUICK REFERENCE

- Develop strategic evaluation frameworks that assess technologies across threat mitigation value, throughput efficiency, and employee experience
- Conduct comprehensive technology assessments through pilot testing and operational validation
- Test equipment in actual environmental conditions before full deployment
- Perform total cost of ownership analyses that extend beyond initial purchase price
- Negotiate comprehensive service agreements during procurement
- Establish preventive maintenance and calibration programs
- Consider purchasing spare units for maintenance rotation to maintain continuity of operations during equipment failures
- Plan for technology evolution and maintain upgrade flexibility

SECTION 8: PROHIBITED ITEMS AND TOOLS OF THE TRADE

Aviation workers often require specific tools and equipment to perform their jobs within secure areas, creating unique policy and procedural requirements that differ from passenger screening frameworks. Establishing comprehensive policies for prohibited items and managing tools-of-trade authorizations requires airports to create frameworks that define clear security boundaries while enabling essential work activities. These policies represent one of the most significant operational distinctions between employee and passenger screening programs.

8.1 Developing Prohibited Items and Tools-of-Trade Management Policies

This section examines how airports develop prohibited items policies and tools-of-trade authorization systems, and includes research findings on list development approaches, authorization processes, discovery procedures, and documentation practices. Unlike passenger screening where prohibited items are universally restricted, full employee screening must balance security requirements with the operational realities of a diverse workforce: airport construction contractors, maintenance personnel, airline ramp agents, and others who may require specific tools and equipment to perform their jobs within airport secure areas. These policies serve several important functions: defining clear boundaries for acceptable items, establishing accountability mechanisms for authorized tools, providing consistent enforcement procedures, creating legally defensible frameworks, and ensuring clear notice to employees about prohibited items and authorization processes.

8.1.1 Prohibited Items List Development

The research revealed that Prohibited Items Lists are typically developed by using the TSA's list of items prohibited in airport Sterile Areas, as found on their website: <https://www.tsa.gov/travel/security-screening/whatcanibring/all-list>. The TSA Prohibited Items List provides comprehensive categories including weapons, explosives, incendiaries, sharp objects, blunt instruments, chemical substances, and other items deemed hazardous. Some airports noted allowing liquids through employee portals as their only major deviation from the TSA list, while others built in flexibility for specific positions while staying close to the TSA baseline.

Many of the interviewed airports incorporate disclaimer language into their prohibited items policies, stating that lists are not exhaustive and that airports retain discretion to prohibit additional items deemed dangerous or inappropriate. This approach provides security personnel with necessary flexibility to address novel threats or items not explicitly listed while maintaining clear baseline standards and providing clear notice to employees.

8.1.2 Tools-of-Trade Authorization and Accountability Processes

The research revealed significant diversity in how airports approach tools-of-trade authorization and accountability. Approaches ranged from highly formalized permit systems with digital tracking to discretionary judgment-based assessments conducted at screening checkpoints. The diversity in approaches reflects the different paths airports have taken as they have developed and refined their practices through operational experience rather than adherence to any standardized model.

A tool of the trade refers to a tool that would otherwise be prohibited at a full employee screening checkpoint but is necessary for an aviation worker to perform their job in an airport's Secured or Sterile

Area.⁴⁶ Examples include multi-tools, wrenches, saws, concession knives, box cutters, and other implements required for maintenance, construction, or concessions. Regardless of the authorization approach an airport adopts, certain principles apply universally. Tools of the trade are not accessible to the public and remain under the visual and physical control of the authorized individual at all times. An employee ceases to have control of a tool if they allow it to be accessed or used by a person for whom it is not authorized.

The operational and financial implications of a tool of the trade found unsecured in the Secured or Sterile Area can be severe. Depending on the circumstances, consequences could include evacuation of the Sterile Area, aircraft delays, potential litigation in response to significant financial losses for stakeholders and customers, TSA enforcement actions, and reputational damage. These potential consequences underscore the importance of implementing robust authorization, accountability, and compliance monitoring processes for tools of the trade.

FORMAL AUTHORIZATION SYSTEMS

Airports across the study implemented structured authorization processes requiring advance approval before employees can bring tools into Secured Areas, with varying levels of complexity. These systems typically include application processes, documentation requirements, and verification procedures at screening points.

- **Permit-Based Systems:** Some airports require employees to carry a permit or license issued by the airport authority for each tool or category of tools they need for their work. Under these systems, employees must apply for authorization, which is reviewed by security personnel who assess the operational need. If approved, the employee receives documentation (such as a permit card) that must be presented at screening alongside the tools themselves. This approach creates accountability by linking specific individuals to specific authorized items, while providing screeners with clear guidance on what to allow.
- **Badge Endorsement Systems:** One international airport incorporates tools-of-trade authorization directly into their badging process. Under this approach, authorization is tied to the individual's role and vetted by the airport. Employees receive endorsements for specific categories of tools (such as multi-tools, wrenches, saws, concession knives, box cutters, or aerosol cans) that appear on their credentials. At full employee screening checkpoints, items are screened as normal, then allowed through if the employee's credential shows the appropriate endorsement. This system includes expiration dates requiring periodic renewal.
- **Digital Tracking Systems:** One international airport developed an in-house software system that manages tool authorization through an online application process. Airport employees and contractors submit applications with tool details and photographs, and approved tools receive QR codes that are scanned each time the tools are brought through entry and exit of airport secure areas. Security staff equipped with tablets verify each tool against the database photos, with tools matching exactly or entry being denied. Exit verification ensures all tools are accounted for, with the system generating warnings for non-compliance. This approach replaced a paper-based process and significantly improved stakeholder acceptance due to faster processing times.

PERIODIC VERIFICATION REQUIREMENTS

Rather than one-time authorization, some airports require ongoing verification of tools-of-trade status. One airport changed its process to require monthly reapplication and reauthorization to remain on the

⁴⁶ Many such items, including bladed tools, sharp objects, and tools that are longer than seven inches, are prohibited or restricted at TSA passenger screening checkpoints. TSA, "What Can I Bring?," accessed January 16, 2026, <https://www.tsa.gov/travel/security-screening/whatcanibring/all>.

approved tools list, recognizing that operational need is not permanent. Construction projects begin and end, workers move to different areas, and the tools required for specific jobs change over time. This approach allows the airport to verify that authorization remains valid rather than maintaining generic lists that may become outdated.

DISCRETIONARY AND JUDGMENT-BASED APPROACHES

Many of the airports interviewed rely on screener discretion and supervisor support rather than formal permit systems. Under these approaches, screeners assess tools-of-trade authorization at the point of screening based on factors such as:

- Badge type and job function verification
- Conversation with the employee about their work
- Visual assessment of whether appearance and equipment are consistent with the stated role
- Confirmation that work is actually occurring in the area the employee is accessing
- Supervisor consultation for questionable items

Security contractors emphasized the importance of clear escalation procedures under discretionary approaches, with one contractor noting their policy: “if you have any doubt, then there’s no doubt—call it.” Airports using discretionary approaches typically provide training on common tools of the trade with examples, while maintaining that operations personnel make final determinations on questionable items.

TOOL ACCOUNTABILITY MECHANISMS

Beyond authorization, airports implement various mechanisms to maintain accountability for tools once they enter secure areas.

- **Tool Engraving:** One airline requires all tools to be engraved with employee numbers, with engravers available at checkpoints when setting up new locations. This practice enables identification of ownership if tools are found unattended and creates individual accountability. Advance notification is sent about engraving requirements, and most employees arrive with pre-engraved tools.
- **Entry and Exit Matching:** Some airports require employees with tools to complete an inventory list upon entry that is matched against tools upon exit. This establishes accountability throughout the screening process and helps ensure no tools are left behind in secure areas. One airport noted this approach is particularly important for contractors working under time-limited projects.
- **Tool Storage in Secure Areas:** Several airports encourage or require contractors to maintain toolboxes or storage within the secure area once tools are initially screened, reducing the need for repeated screening of the same items. One international airport specifically encourages subcontractors to establish offices within the security restricted area to store tools, noting that tools brought in once can remain in place rather than being screened repeatedly.
- **Concession Tool Logs:** Airports with food service and retail concessions often require these businesses to maintain tool logs documenting kitchen knives and other sharp items. One airport requires concession knives to be engraved by the airport and audited monthly, with items required to remain on premises.

PROACTIVE COORDINATION APPROACHES

Several airports in our study emphasized communication with stakeholders as central to their tools-of-trade approach rather than relying solely on screening-point decisions. One airport conducts weekly construction project meetings specifically to discuss needed tools, providing proactive communication

about upcoming work and educating new vendors on requirements. Pre-construction meetings before project start help establish expectations and reduce screening delays.

TRAINING AND ACKNOWLEDGMENT REQUIREMENTS

Aviation workers who are approved to carry tools of the trade may require training on their responsibilities as authorized tool holders. Training programs observed in the research address topics such as:

- Secure handling and storage procedures within the Secured or Sterile Area
- The requirement to report lost or missing tools immediately
- Recognizing and preventing potential misuse of tools
- Consequences if handling requirements are violated

Some airports require aviation workers to provide written acknowledgment confirming they understand their responsibilities before receiving tools-of-trade authorization. These acknowledgments typically address requirements such as maintaining a written inventory of authorized items, ensuring items are required for the job currently being performed, maintaining control and accountability of items at all times, keeping items locked, secured, or within sight when not in use, and storing items in an area secured with a lock when not being actively used. Written acknowledgments also typically specify that violations of security procedures identified during compliance checks or audits will be documented and may result in a security citation or loss of access privileges.⁴⁷

ENFORCEMENT CONSIDERATIONS

Effective tools-of-trade management requires ongoing compliance monitoring to verify that authorization processes are functioning as intended and that aviation workers are adhering to requirements. Compliance activities observed in the research include random inspections of tools carried by aviation workers to verify against authorizations, assessment of inventory records and permit issuance logs, review of tenant tool registers at concessions and food service operations, and verification that security personnel understand tools-of-trade procedures during quality assurance evaluations. These proactive monitoring activities complement the broader quality assurance practices addressed in *Section 11.1*.

Tools-of-trade policies also require enforcement mechanisms to address violations and maintain program integrity. Approaches observed in the research include:

- Automated notifications to airport tenants and contractors when employees are non-compliant with tool verification requirements
- Badge suspension for serious or repeated violations
- Denial of future tool authorization requests for non-compliant individuals
- Warning systems with escalating consequences for violations
- Tracking systems that flag employees who abandon screening to detect potential circumvention through other access points

PARAS 0060 *Strategies for Developing an Aviation Worker Screening Program* provides sample forms and visual examples that airports may find useful when developing tools-of-trade management processes, including a sample prohibited items permit application, sample instructions for tools-of-trade

⁴⁷ For additional guidance on tools-of-trade management principles, see Neil Trethewey et al., *Strategies for Developing an Aviation Worker Screening Program*, PARAS 0060 (Washington, DC: National Safe Skies Alliance, Inc., July 2024), Section 6.2.

holders, a sample tool register for tracking tools within the Sterile Area, and an example of a tools-of-trade endorsement icon for airport ID media.⁴⁸

8.1.3 Prohibited Items Discovery Procedures

When prohibited items are discovered during screening, the airports surveyed typically follow detailed procedures outlined in their SOPs and Post Orders. These procedures include immediate steps for securing the item, notifying the security operations center, documenting the discovery, and determining appropriate disposition. Many research airports provide employees with opportunities to return non-dangerous prohibited items to non-screened locations such as vehicles or landside offices rather than immediate confiscation. This approach recognizes that employees may inadvertently bring prohibited items to screening checkpoints and provides a reasonable resolution that maintains security while avoiding unnecessary punitive measures.

For discoveries involving firearms, tactical knives, pepper spray, or other dangerous items, standard practice among interviewed airports involves mandatory escalation to law enforcement, although the specific response varies by item type and airport. These discoveries may also warrant mandatory badge suspensions or revocations. Clear escalation criteria should distinguish between inadvertent policy violations and potential security threats, ensuring appropriate responses to different categories of prohibited items discoveries. One airport uses a graduated violation system with escalating penalties based on severity. Security contractors noted significant inconsistencies between airports in how prohibited item discoveries are handled and escalated.

DOCUMENTATION AND TRACKING SYSTEMS

Documentation practices for prohibited item discoveries varied across the airports in the study. Most airports maintain some form of records for prohibited item discoveries, including item descriptions, circumstances of discovery, individuals involved, and ultimate disposition. These records serve multiple purposes: supporting regulatory compliance demonstrations, enabling trend analysis to identify recurring issues, providing evidence for potential enforcement actions, and informing training and policy updates based on operational experience. Security contractors emphasized the importance of keeping detailed records regardless of whether assistance is called, noting this documentation supports both accountability and continuous improvement.

8.2 Recommendations and Implementation Guidance

1. ESTABLISH COMPREHENSIVE PROHIBITED ITEMS LISTS

Develop clear prohibited items policies that provide baseline security standards, include disclaimer language allowing flexibility to address novel threats, and ensure clear notice to employees about prohibited items.

Implementation Guidance: Begin with TSA’s list of items prohibited in the Sterile Area as the foundation. For airports with unique operational needs, consider whether separate lists for Secured versus Sterile Areas would be beneficial. Incorporate a statement clarifying that the prohibited items lists are intended as guidance and may not cover every possible scenario, granting security personnel the discretion to restrict additional items as needed. Ensure employees receive clear notice about prohibited items through signage, training, and regular communications. Review and update lists based on operational changes and lessons learned from incidents.

⁴⁸ Ibid., Appendix A (Prohibited Items Permit Application) and Figures 6-2 through 6-4.

2. IMPLEMENT A FORMAL TOOLS-OF-TRADE AUTHORIZATION SYSTEM

Create structured processes for evaluating, approving, and tracking tools-of-trade authorizations that accommodate both security requirements and operational necessities.

Implementation Guidance:

- **Authorization Process:** Consider developing application or declaration forms that capture necessary information about requested tools of the trade, including worker identification, tool type and description, operational purpose, and estimated duration of use. Establish clear criteria for reviewing and approving requests, such as legitimacy of the operational purpose, availability of alternative non-threatening tools, and the applicant's past security record. For airports seeking enhanced accountability, consider implementing a badge identification system with icons or endorsements indicating tools-of-trade authorization, enabling quick verification during screening. Airports interested in comprehensive tracking may consider implementing digital systems with QR codes or similar technology for tracking tools from entry through exit.
- **Accountability and Compliance:** For airports implementing formal authorization systems, consider requiring aviation workers to complete training on their responsibilities as authorized tool holders, covering topics such as secure handling and storage procedures, the requirement to report lost or missing tools immediately, and consequences for violations. Requiring a written acknowledgment signed by the aviation worker confirming understanding of these responsibilities creates documentation that supports enforcement actions if violations occur. Compliance monitoring activities may include random inspections of tools carried by aviation workers to verify against authorizations, periodic assessment of inventory records and permit issuance logs, and review of tenant tool registers at concessions and food service operations. For sample forms including a prohibited items permit application, tools-of-trade instructions, and a tool register, see PARAS 0060 *Appendix A* and Figures 6-2 through 6-4.⁴⁹

3. CREATE CLEAR RESPONSE PROTOCOLS FOR PROHIBITED ITEM DISCOVERIES

Develop clear procedures for addressing prohibited item discoveries that differentiate between inadvertent violations and potential security threats.

Implementation Guidance: Establishing clear and effective response protocols for prohibited item discoveries is essential to maintain airport security and operational integrity. The following recommended practices outline key steps for security personnel and airport management to ensure consistent and compliant responses to these incidents:

- Conduct a thorough assessment to determine if both the individual and the item are authorized, taking into account operational needs such as the person's role, the item's intended use, the person's work area, and approved access zones.
- Establish clear procedures for promptly notifying the airport Security Operations Center when prohibited items are discovered.
- Secure all discovered items and provide employees with options for the voluntary return of non-dangerous items to vehicles or non-secure locations.
- Require law enforcement notification for discoveries involving firearms or other dangerous prohibited items.

⁴⁹ Ibid.

- Coordinate with law enforcement to identify which items may be prohibited and illegal in the jurisdiction. For example, laws regarding pocketknife blade length, automatic opening, gravity deployment, and concealment vary by jurisdiction.
- Consider implementing a graduated enforcement system, such as badge suspensions or revocations, that reflects the frequency and severity of offenses, while adapting procedures to your airport's specific operational context.

4. IMPLEMENT DOCUMENTATION SYSTEMS FOR COMPLIANCE AND IMPROVEMENT

Establish documentation practices that support compliance and enforcement of airport security rules and regulations, while enabling continuous improvement.

Implementation Guidance: Develop standardized documentation forms for prohibited item discoveries and dispositions. Airports implementing large-scale full employee screening programs should consider adopting electronic systems to enable efficient verification and robust audit support. Use documentation to identify trends and recurring issues that can inform training updates and policy improvements. Maintain records in accordance with regulatory requirements.

SECTION 8 QUICK REFERENCE

- Establish comprehensive prohibited items lists with clear employee notice
- Implement formal authorization systems for tools of the trade
- Create well defined response protocols for prohibited items discoveries
- Maintain documentation systems for compliance and improvement

SECTION 9: OPERATING PROCEDURES

Developing comprehensive operating procedures is essential for translating screening policies into consistent daily operations. These procedures provide screening personnel with clear, step-by-step guidance for conducting screening activities, resolving alarms, responding to incidents, and documenting operational events.

9.1 Establishing Operating Procedures

This section examines how airports develop SOPs for full employee screening, including alarm resolution protocols, incident response frameworks, documentation requirements, and maintenance practices. Operating procedures form the backbone of daily screening operations, requiring careful consideration of airport-specific factors such as infrastructure constraints, staffing models, regulatory requirements, and stakeholder needs. Building on the prohibited items policies and tools-of-trade framework established in *Section 8*, operating procedures must address how these policies are implemented during daily screening operations. The complexity of developing effective operating procedures stems from the need to consider multiple competing priorities:

- Maintaining robust security while minimizing operational disruption
- Ensuring consistent application while allowing flexibility for unique situations
- Creating legally defensible processes while maintaining positive employee relations

These procedures serve dual purposes as both the basis for training screening personnel and potential evidence in legal claims or complaints. This makes their proper development and documentation essential for the success of an airport's full employee screening program.

9.1.1 SOP Development Approaches

Approaches to SOP development vary based on governance structures and available resources. Comprehensive SOPs can be developed entirely in-house, detailing step-by-step procedures for magnetometer use, AIT operation, x-ray and ETD screening for accessible property, and specific protocols for alarm resolution. Alternatively, SOP development can be delegated to security contractors, with airport personnel reviewing and approving procedures with minor modifications. Existing TSA SOP models also serve as effective foundations, with screening procedures adapted from TSA Standard Security Programs or other screening SOPs to meet specific operational needs.

Most airports involved one or more stakeholder groups in their SOP development processes, such as airport law enforcement, security contractors, TSA representatives, and major tenants. One international airport described an iterative development process involving initial SOP development by the security contractor, procedure creation by the security contractor, compliance review by airport security personnel, testing with contractors and frontline staff, gathering feedback, adjustments, and final validation testing—although this comprehensive approach may not be feasible for all procedures airports develop.

9.1.2 SOP Content and Structure

The airports surveyed typically structured their SOPs to address routine screening operations, special circumstances, prohibited items, tools-of-trade management, alarm resolution, and escalation procedures. SOPs in the research sample commonly included detailed procedures covering equipment operation, prohibited item identification, screening techniques, documentation requirements, and

customer service interactions. Procedures should incorporate “human aspects,” recognizing that security personnel must manage various personality types and situations where security may not be employees’ primary concern when arriving for work. The level of detail varied, with some airports developing comprehensive step-by-step instructions for each screening technology while others maintained more general procedural guidelines.

Robust business continuity and contingency planning for various disruption scenarios are essential. One vendor described maintaining an “all hazards” approach to contingency planning, preparing for weather events, equipment failures, and other operational disruptions. Their business continuity plans include specific protocols such as calling in additional employees during emergencies, providing hotel accommodations, and arranging transportation to and from work during severe weather conditions. When equipment failures occur, procedures include transitioning to 100% manual inspection to maintain continuous screening operations. This comprehensive approach ensures screening operations can continue regardless of circumstances, recognizing that airports must maintain security even during extraordinary events.

9.1.3 SOP Relation to ASP

Most airports in this study reported keeping detailed SOPs separate from their ASPs, including only high-level information on the full employee screening program in the ASP itself. This separation strategy was more common among airports with mature full screening programs operating for multiple years. This separation allows airports to make operational modifications and SOP updates without requiring a formal amendment to the ASP. However, approaches varied among the airports studied. One large hub airport incorporated its screening procedures directly into an ASP amendment, including descriptions of screening processes, technologies used, and resolution procedures. Airport officials explained that documenting these elements within the ASP itself could help provide a defense against potential legal or privacy challenges. They emphasized keeping the ASP language general enough to allow operational flexibility while still providing sufficient detail to establish the program’s legitimacy and authority. This helps avoid being locked in to specific protocols that might need to change as new requirements emerge, or new screening technologies are implemented. This approach recognizes that for some airports, documenting screening operating procedures in the ASP may serve as important evidence in legal proceedings, demonstrating the airport’s employee screening procedures are carried out in compliance with Federal regulatory requirements.

For guidance on when ASP documentation may be required despite preference for separation, see Section 12.1.

9.1.4 SOP Maintenance and Updates

Among the airports interviewed, regular SOP review and updates were identified as essential for maintaining effectiveness, ensuring that SOPs align with changes to the threat and operating environment, and reducing knowledge gaps among the screening staff. Regular procedure reviews help refine operations to enhance security effectiveness, improve throughput, and incorporate lessons learned from other airports. For example, one airport described multiple iterations of their alarm resolution procedures to address operational challenges. Initially, they conducted pat-downs followed by rescreening the individual through the metal detector. However, due to volume concerns during peak times causing significant delays in secondary screening, they revised their approach. The airport ultimately implemented a streamlined process where if a person alarms, they must divest and go back through; if they alarm a second time, they receive ETD swab and handheld metal detector screening; and if the alarm still cannot be resolved, the employee is referred to TSA. This evolution demonstrates how

airports must balance security requirements with operational efficiency, particularly during high-volume periods.

Other airports in the research described dedicating specific staff members to handle SOP and training updates, adapting SOPs based on assessments of operational performance and security incidents over time. The research findings indicate that most airports in the study treat SOPs as living documents that evolve based on operational experience, security incidents, regulatory changes, and emerging threats. However, when there are multiple changes to SOPs, effective administration and version control become increasingly important to ensure that the most current procedures are being utilized and that updated information is shared promptly with all relevant stakeholders.

9.1.5 Alarm Resolution Processes

Airports in the research described multi-step alarm resolution processes, typically allowing employees one to three attempts to clear alarms through additional divestment before escalation. This approach helps reduce unnecessary escalations while maintaining security effectiveness.

PAT-DOWN PROCEDURES AND LIMITATIONS

The research revealed significant variation in pat-down approaches, with many expressing concerns about legal liability. Several airports in the study have implemented “no-touch” policies, avoiding pat-downs entirely and instead directing unresolved alarms to alternative resolution methods.

Among airports that permit pat-downs, detailed procedures typically specify who may conduct them, acceptable techniques, and applicable limitations. Standard procedures include:

- Pat-downs limited to non-sensitive areas (avoiding crotch, breast, and buttocks)
- Verbal consent required before any physical contact
- Authorization limited to supervisors or designated security personnel
- Back-of-hand technique for non-sensitive area searches
- Private screening areas available when requested

For legal considerations regarding pat-down liability and alternative approaches, see Section 13.1.4.

GENDER-SPECIFIC STAFFING REQUIREMENTS FOR PAT-DOWN PROCEDURES

Airports conducting pat-downs face operational requirements for gender-specific staffing to enable same-gender screening. One large Category X airport initially maintained a 50/50 male/female staffing ratio to ensure adequate coverage for gender-specific pat-downs. However, as technology solutions reduced the need for physical pat-downs, this airport adjusted to approximately 70/30 male/female ratio while still meeting operational requirements. Another airport using contractors includes contractual requirements for both male and female staff presence at all times to ensure gender-appropriate screening capability. These gender-specific staffing needs represent operational requirements that apply regardless of whether airports use direct employees, contractors, or hybrid staffing models discussed in *Section 10.1 Staffing Model Considerations*.

SPECIAL ASSISTANCE AND MEDICAL ACCOMMODATIONS

The research revealed consistent approaches for accommodating employees with disabilities or medical conditions. Most airports direct employees who cannot use standard screening equipment due to medical devices, pacemakers, or other conditions to TSA passenger checkpoints where trained personnel can provide appropriate alternative screening. Several airports have developed specific protocols for these

situations, including private screening areas when requested along with modified procedures that maintain security while respecting dignity and privacy.

For employees with prosthetics or medical implants, alternatives to magnetometer screening are typically offered, such as visual inspections or limited pat-downs of non-sensitive areas. Religious accommodations, such as self-pat procedures for head coverings followed by ETD of the hands, were also reported among several airports. Most airports emphasized that these accommodations are handled on a case-by-case basis, with security supervisors trained to make appropriate determinations while maintaining security standards.

ESCALATION PATHWAYS

The most common escalation approach among surveyed airports involves directing employees with unresolved alarms to TSA passenger screening checkpoints for additional screening. At least ten airports confirmed relying on TSA checkpoint referral as their primary or alternative method for alarm resolution. Several airports also emphasized the critical importance of maintaining chain of custody during these escorts, ensuring continuous supervision of the employee from the initial screening point to the TSA checkpoint to prevent any security breaches or attempts to circumvent the screening process. One airport in the study uses a formal documentation system for employees with unresolved alarms. Employees are given a form and directed to a TSA checkpoint; once the process is complete, the forms are collected to verify compliance. The choice to rely on TSA checkpoint referrals for unresolved alarms, while simplifying procedures and reducing potential liability, may create regulatory documentation requirements depending on local TSA interpretation.

For ASP documentation implications of TSA checkpoint referrals, see Section 12.1.2. For liability considerations in choosing escalation methods, see Section 13.1.

For certain alarm types or prohibited item discoveries, a significant number of airports involved in the study established direct escalation to the Security Operations Center or airport law enforcement. Security vendors emphasized keeping detailed records whether they call for assistance or not, noting differences between airports with dedicated airport police departments versus those with city/county police coverage. Airports with dedicated police departments typically require notification for all prohibited item discoveries, while some city/county departments prefer not to be called for minor incidents.

One airport implemented a system for temporary confiscation of airport badges for employees denied entry due to unresolved alarms, particularly during after-hours periods when TSA checkpoints are unavailable to assist with alarm resolution. In these situations, the individual is escorted from the secure area without their badge, and the badge is securely stored until it can be properly addressed by security personnel the next business day. This practice prevents unauthorized access while maintaining security integrity during off-peak hours.

9.1.6 Incident Response Protocols

The research identified common incident types requiring response protocols: discovery of prohibited items, employee screening refusal, unresolved alarms, unauthorized personnel identification, suspicious behavior during screening, and access control or perimeter breaches. Most airports in the study emphasized the importance of clear, step-by-step protocols that minimize confusion and ensure consistent incident handling. Response protocols among surveyed airports typically incorporate five key elements to ensure consistent incident handling for each type of event: initial assessment and containment procedures, clear communication and notification guidelines, specific escalation criteria and thresholds, evidence preservation requirements, and formal resolution and closure steps. These

elements provide structured frameworks for security personnel to follow during various incident scenarios.

9.1.7 Documentation and Reporting Requirements

Among the airports interviewed, documentation practices varied significantly, with most emphasizing the importance of maintaining records to support regulatory compliance and investigations. For airports that confiscate badges when alarms cannot be resolved after hours, it is important to document each incident thoroughly. This includes recording key details about the event, securing the badge until proper review, and outlining clear steps for returning the badge and conducting an incident review the following business day. Integrating CCTV footage into the documentation process helps ensure a comprehensive and verifiable record of what occurred. Use of CCTV with audio can add details for documenting security violations and reduce the likelihood of false reporting. Camera coverage requirements have become standard practice at many of the airports involved in the study, with several implementing strategic positioning, including cameras over search tables to document search procedures, protect staff from false allegations, and ensure compliance with established protocols.

A small number of airports in the research have begun implementing digital documentation approaches for their screening operations, including one international airport with a comprehensive digital documentation system, one domestic airport maintaining digital logs for screening exceptions and prohibited items, and another domestic airport using cameras and integrated technology to capture operational data for reporting. These digital approaches are not yet widespread in industry. Among airports with some level of digital documentation, specific applications vary. For example, some airports maintain tracking systems for accommodation requests, documenting when employees require alternative screening methods due to medical conditions or disabilities. This documentation ensures consistent application of procedures while maintaining privacy requirements and enables airports to identify patterns in accommodation needs. Despite these practices, comprehensive enterprise-wide documentation and reporting systems were not a primary focus of discussion among most airports, suggesting this remains an area for potential development as full employee screening programs mature.

9.2 Recommendations and Implementation Guidance

1. DEVELOP COMPREHENSIVE SOPS USING STAKEHOLDER INPUT

Establish detailed SOPs through collaborative development involving TSA representatives, security teams, security screening personnel and contractors, law enforcement, or other major stakeholders to ensure procedures are practical, compliant, and address all operational needs.

Implementation Guidance: To develop effective SOPs, airports should follow these key steps:

- Assemble a cross-functional team including airport security, operations, legal counsel, law enforcement, and key tenant representatives to lead SOP development.
- Review existing models such as airline screening procedures or TSA program templates as starting points, then tailor them to meet airport-specific needs.
- Structure SOPs with clear, step-by-step instructions covering routine operations, special circumstances, handling of prohibited items, and escalation protocols.
- Conduct pilot testing with frontline staff prior to full implementation, and use their feedback to refine procedures.
- Maintain SOPs as separate documents from the ASP to allow operational flexibility; include only high-level information in the ASP to minimize amendment requirements.

2. IMPLEMENT MULTI-TIERED ALARM RESOLUTION PROTOCOLS

Design alarm resolution procedures that provide multiple opportunities for non-intrusive resolution before escalating to more intensive screening methods or access denial.

Implementation Guidance: Establish a “divest-best-test” protocol allowing employees initial opportunities to remove items causing alarms before rescreening. Define specific limits such as three metal detector attempts before requiring alternative resolution. Airports avoiding pat-downs due to liability concerns should develop clear alternative procedures such as TSA checkpoint referral or law enforcement involvement. If pat-downs are permitted, create detailed protocols specifying authorized personnel, acceptable techniques, gender-specific requirements, and medical accommodation procedures. Implement formal documentation systems for checkpoint referrals, using tracking forms to ensure compliance when employees are directed to TSA screening. For after-hours situations when TSA checkpoints are not available, consider implementing badge confiscation protocols with clear procedures for incident documentation.

3. CREATE STRUCTURED INCIDENT RESPONSE FRAMEWORKS

Develop clear incident response protocols addressing common scenarios with defined roles, escalation criteria, and documentation requirements.

Implementation Guidance: Identify and categorize common incident types including prohibited item discovery, screening refusal, unresolved alarms, unauthorized access attempts, and suspicious behavior. For each category, establish five-step response protocols covering initial assessment and containment, notification requirements and communication chains, specific escalation thresholds and criteria, evidence preservation procedures, and formal resolution and closure processes. Define clear notification matrices specifying which personnel or agencies must be contacted for different incident severity levels. Create incident-specific checklists or job aids for security personnel to ensure consistent response across all shifts. Establish evidence preservation protocols including securing physical items, preserving video footage, and maintaining chain of custody documentation.

4. ESTABLISH CLEAR PROTOCOLS FOR SPECIAL ASSISTANCE AND MEDICAL ACCOMMODATIONS

Develop comprehensive procedures for screening employees with disabilities, medical conditions, or religious accommodation needs that maintain security while ensuring dignity and compliance with ADA requirements.

Implementation Guidance: Create standardized protocols for common accommodation scenarios, including employees with medical implants, prosthetics, or mobility devices. Establish partnerships with TSA for security checkpoint personnel to handle complex medical screenings when necessary. Train security supervisors on appropriate accommodation determinations and privacy requirements. Where feasible, larger airports may want to consider developing private screening for sensitive situations. Consider religious and cultural sensitivities in developing alternative screening procedures, such as self-pat options with ETD verification.

5. ESTABLISH REGULAR SOP REVIEW AND UPDATE CYCLES

Implement a regular process for reviewing and updating SOPs based on operational experience, incidents, and lessons learned from other airports.

Implementation Guidance: Schedule periodic SOP reviews involving security management and frontline personnel to identify needed updates or clarifications. Create formal processes for incorporating lessons learned from security incidents, operational challenges, or regulatory changes into procedure updates. Develop version control systems to track changes and ensure all personnel have access to current procedures. Implement feedback mechanisms allowing frontline staff to suggest

improvements based on operational experience. Coordinate SOP updates with training programs to ensure personnel receive timely instruction on procedure changes.

6. IMPLEMENT COMPREHENSIVE DOCUMENTATION AND REPORTING SYSTEMS

Establish documentation practices for all screening activities with integrated reporting mechanisms for regulatory compliance and continuous improvement.

Implementation Guidance: Define minimum documentation requirements for routine screening operations, security incidents, prohibited items discoveries, alarm resolutions, and special accommodation requests. Develop standardized forms and templates ensuring consistent information capture across all documentation. For larger airports implementing full employee screening programs, consider technology solutions such as electronic incident reporting systems or mobile applications to streamline documentation processes. Create notification protocols specifying which personnel or agencies must be contacted for different incident severity levels.

7. DEVELOP BUSINESS CONTINUITY PLANS FOR SCREENING OPERATIONS

Create comprehensive contingency plans to address scenarios such as equipment failures, weather events, and other disruptions to maintain continuous screening capability.

Implementation Guidance: Develop scenarios for common disruptions including power outages, equipment failures, severe weather, and security incidents. Establish fallback protocols, such as transitioning to 100% manual inspection during power outages or when technology fails. Document lessons learned from actual disruptions to continuously improve response capabilities.

SECTION 9 QUICK REFERENCE

- Develop comprehensive SOPs through stakeholder collaboration, maintaining them separately from ASPs for operational flexibility
- Implement multi-tiered alarm resolution processes minimizing intrusive measures and liability exposure, while maintaining security
- Create structured incident response frameworks with defined escalation criteria and documentation requirements
- Conduct regular SOP reviews that incorporate lessons learned and operational feedback
- Establish documentation systems for incidents, accommodation requests, and regulatory compliance

SECTION 10: WORKFORCE MANAGEMENT

Effective workforce management represents the foundation of any successful full employee screening program. Unlike technology and infrastructure investments that remain relatively static once implemented, workforce management requires continuous attention and adaptation to maintain program effectiveness and respond to evolving operational needs.

Staffing decisions shape every aspect of full employee screening program operations, from implementation timelines to long-term sustainability. How airports staff and manage their screening workforce fundamentally determines program costs, quality control mechanisms, and operational flexibility.

10.1 Staffing Model Considerations

This section examines how airports select and manage staffing for full employee screening operations, including the three primary staffing models, data-driven scheduling approaches, and strategies for recruitment and retention. Airports must consider whether to use direct employees, contract security personnel, or a hybrid approach. This process involves assessing factors such as cost implications, implementation timelines, staffing flexibility, liability concerns, and how well the model integrates with existing security functions at the airport. Each approach offers distinct advantages and challenges that must be assessed against the airport's specific circumstances, governance structure, available resources, and organizational priorities. Additionally, airports must address recruitment and retention challenges while establishing sustainable staffing levels and scheduling approaches that harmonize security requirements with operational efficiency.

10.1.1 Direct Airport Employee Model

Several airports interviewed staff their employee screening operations with direct airport employees. Airports utilizing direct employees cited advantages including greater control over performance quality, ability to maintain consistent customer service standards, and better integration with broader security operations and culture. One large Category X airport implementing full employee screening uses all direct employees, emphasizing this aligns with the airport's commitment to job creation. The airport noted advantages including good employee benefits through collective bargaining agreements and being part of the unified airport team.

One Category I airport transitioned from contractors to direct employees after experiencing reliability and cost challenges. This airport, which does not conduct full employee screening, hired dedicated Public Service Officers under the police department's authority. These officers perform AWS alongside other security duties such as traffic monitoring, parking enforcement, merchandise inspections, and random security checks. While this airport's experience is with random continuous AWS, the considerations about direct employees performing multiple security functions remain relevant for airports considering full employee screening.

Despite these advantages, airports using this model generally noted challenges including higher personnel costs due to benefits and equipment, staffing difficulties during vacations and leave periods, and scheduling complexities. One airport noted that city hiring processes can be extremely lengthy, with positions potentially taking several months to fill, making direct employee models less responsive to changing operational needs. Additionally, a Category X airport using direct employees also operates under strict collective bargaining agreement guidelines, which can add complexity to staffing decisions and operational flexibility.

Table 4. Direct Airport Employee Staffing Model

Advantages	Disadvantages
• Greater control over quality and performance – Direct oversight of screening operations and performance • Better integration with airport operations and culture – Employees are part of the airport team, are more familiar with airport operations, and understand organizational priorities • Consistent customer service standards – Direct employees can better maintain airport's service philosophy and approach • Multifunctional workforce capability – Can perform various security duties beyond screening (parking enforcement, vehicle gate inspections, etc.) and be redeployed during non-peak periods • Long-term retention potential – Several airports reported higher retention rates with direct airport employees benefitting from more established airport career paths • Direct accountability and authority – Clear chain of command within the airport for security decisions	• Higher personnel costs – Benefits, equipment, training, and long-term employment obligations • Extended hiring timelines – City/government hiring processes can take several months • Staffing coverage challenges – Difficulties managing vacations, training, sick leave, and shift changes • Limited flexibility for scaling – Harder to adjust staffing levels for changing operational needs • Budget approval – Obtaining budget approval is a significant disadvantage, as securing necessary funding for direct airport employee staffing can be lengthy and complex, and requires extensive coordination among multiple stakeholders • Administrative burden – Airport manages all HR functions including recruitment, training, discipline

10.1.2 Security Contractor Model

The majority of airports in this research reported using security contractors for full employee screening operations. Airports frequently cited several factors influencing their decision to use contractors: quicker implementation timeframes; cost considerations (particularly avoiding long-term benefit obligations); specialized security experience; staffing flexibility to adjust to changing needs; liability management and risk sharing; difficulty creating, funding, and sourcing new airport positions; and union considerations.

One airport implementing AWS demonstrated an innovative contracting approach using tiered staffing levels with differentiated pay rates based on decision-making responsibility, knowledge, training, and skill requirements. Personnel operating specialized x-ray and ETD equipment received higher compensation than those performing basic screening functions. The concept may be particularly applicable to large airports implementing full employee screening, where the scale and complexity of operations could justify differentiated roles and compensation structures to improve retention and performance.

Airports utilizing contractors also face several ongoing challenges, including high turnover rates with challenges sourcing qualified personnel, patterns of staff “training and leaving,” inconsistent experience and competency levels that require frequent retraining, and heightened demands for quality control and oversight. Additionally, maintaining effective communication between airport staff and contract personnel remains a persistent concern. One airport reported that their existing city contract was “written more for securing our buildings downtown” and lacked the specific training qualifications and performance standards needed for aviation security, leading them to plan a new procurement specifically tailored to employee screening requirements. Another challenge noted was that when using existing

municipal contracts, airports may lack authority to enforce performance standards if the contract was not originally designed for aviation security purposes.

One airport's approach to contractor management demonstrates how detailed contract provisions can strengthen oversight and accountability. This major airport incorporated over 40 specific fines and penalties for non-compliance into their security services contract, ranging from warnings to \$1,000 for repeated violations. Violations can include being on phones while on post, submitting late or incomplete reports, and other performance deficiencies. This airport emphasized that having detailed contract requirements with enforcement mechanisms is crucial because without proper mechanisms, airports are unable to directly enforce performance standards and accountability. The focus should be on compliance with clear upfront expectations that allow airports to maintain control over performance standards and training. Some airports have also split security contracts between multiple vendors to improve oversight, although this increases administrative responsibilities.

Table 5. Security Contractor Staffing Model

Advantages	Disadvantages
• Faster implementation – Can deploy screening operations quickly, especially if a security contract is already in place • Cost flexibility – Avoids long-term benefit obligations and can adjust staffing levels more easily • Simplified administration – Contractor handles recruitment, training, HR functions • Reduced liability – Risk sharing with contractor • Specialized expertise – Contractors can bring screening experience from multiple venues and clients, including global expertise • Scalability – Can quickly increase or decrease staffing based on operational needs	• High turnover rates – “Train and leave” patterns reported by multiple airports • Variable experience levels – Continuous need for training due to staff rotation • Quality control challenges – Less direct control over hiring, training, and performance standards • Communication gaps – Increased likelihood of breakdowns between airport staff and contract personnel • Contract limitations – Existing municipal contracts may lack aviation-specific requirements and enforcement “teeth” • Detailed SOP requirements – Need comprehensive written procedures for anticipated operational scenarios

10.1.3 Hybrid Model

Some airports have implemented hybrid staffing models that combine direct employees and contractors. Among the airports surveyed, one Category X airport reported using airport security officers for positions requiring higher levels of knowledge, skills, and decision-making responsibility, while utilizing contractors to supplement staffing, primarily for monitoring x-ray systems at employee screening checkpoints. Direct security officers handle all physical searches, pat-downs, bag resolution, and alarm resolution, serving as the “quarterback” in each screening room, while contractors are limited to operating x-ray belt functions and confirming what the AI software displays. This division allows the airport to maintain authority and quality control over sensitive functions while leveraging contractors for routine monitoring tasks. The airport reported this approach helps control costs and reduce liability while ensuring critical security functions remain under direct airport control.

Another airport using a hybrid model with both contract and airport security personnel at equivalent levels cited a distinct operational advantage: when direct airport employees and contractors perform the same screening functions, the direct employees can immediately identify and correct any misinformation

or training gaps among contract personnel. This real-time quality control is particularly valuable when new contract staff are deployed, as experienced airport employees working alongside them can address procedural errors as they occur and escalate recurring issues to management for correction with the contractor. This peer-level oversight provides an additional quality assurance mechanism unique to hybrid models where both employee types perform identical functions.

In many ways, hybrid models offer airports flexibility to leverage the advantages of both direct employees and contractors while mitigating some of the disadvantages of each approach. This can be particularly valuable for airports transitioning toward full employee screening or managing complex operational environments.

Table 6. Hybrid Staffing Model

Advantages	Disadvantages
• Optimized role allocation – Direct employees handle critical functions while contractors manage routine tasks • Cost efficiency – Balances higher-cost direct employees with lower-cost contractors • Maintained authority and control – Airport retains direct control over sensitive security functions (pat-downs, alarm resolution) • Operational flexibility – Can adjust contractor staffing levels while maintaining core direct employee expertise • Specialized expertise utilization – Direct employees serve as "quarterbacks" while contractors operate equipment • Better quality control – Direct oversight of critical functions with contractor support for volume • Technology adaptation – Allows role specialization as AI and advanced screening technology is implemented	• Complex management structure – Requires coordination between two different workforce types • Training coordination – Must ensure consistent standards and understanding of roles across both employee groups • Multiple oversight requirements – Must manage both employee and contractor performance systems • Communication complexity – Information flow between different employee groups requires active management • Integration challenges – Difficulties building unified team culture across different employment structures

10.1.4 Data-Driven Staffing and Scheduling

The airports involved in this study highlighted the significance of analyzing employee traffic patterns to inform staffing decisions and scheduling for their screening operations. Badge access control data can reveal peak arrival times and traffic volumes, enabling alignment of staffing schedules with actual employee movement patterns. One airport reported that their employee screening checkpoint opens 30 minutes before passenger screening and that security staff scheduling is aligned with employee shift patterns, with multiple screening lanes available to open during peak periods.

One international airport emphasized the importance of coordinating security operations with stakeholder shift patterns. After meetings with various airport entities to understand their shift schedules, the airport implemented a staggered entry system where different companies' employees pass through security checkpoints during designated time windows. For example, security contractor employees pass through from 4:00 to 4:30 a.m. after their shift briefing, while other entities' employees use different

time slots. This staggering system minimizes congestion and delays during peak shift-change periods, though flexibility is maintained for urgent access needs.

10.1.5 Staffing Efficiency and Performance

Research on screening performance indicates that flexible break schedules may be as effective as rigid break rules for maintaining screening effectiveness.⁵⁰ This research found no significant performance advantage for fixed 10-minute breaks compared to alternative or shorter break patterns, suggesting that airports may have more latitude in scheduling—whether using short microbreaks or single longer breaks—as long as total break time is sufficient.

Several airports also emphasized the importance of cross-training screening personnel to perform multiple functions, allowing for more efficient staff utilization. One of the airports interviewed reported that their direct employees perform employee screening alongside various other security duties, maximizing the value of their workforce.

10.1.6 Recruitment and Retention Challenges

Several recruitment challenges have been identified that impact the ability to maintain adequate staffing for screening operations, including:

- Limited candidate pools for security positions
- Comprehensive background check requirements that extend hiring timelines
- Perceptions of limited career growth opportunities
- Competition from other employers offering higher wages
- Extended vetting processes for airport positions compared to other security roles

To address these challenges and improve retention, airports have implemented various strategies. These include creating career progression opportunities and clear advancement paths, developing job rotation programs to expand employee skills and reduce burnout, implementing recognition and reward programs for exceptional performance, establishing competitive compensation structures (particularly for contractor positions), building a positive work culture that values security contributions, and providing ongoing professional development and specialized training.

One airport reported retaining fixed employee screening checkpoint staff for approximately five years by fostering a supportive work environment where screeners were not afraid to make non-critical mistakes and were encouraged to learn and improve from these experiences. The airport emphasized the importance of acknowledging and accepting responsibility when SOP-related issues occurred, rather than placing blame on individual contractors or employees. Strong partnerships between airport security teams and contractors support program effectiveness. Treating contract personnel as an extension of the security team with a “one team, one fight” mentality fosters accountability and collaboration. This approach was reported to improve morale, performance, and retention among contract screening staff.

Some organizations have found that focusing on strong supervision and quality training that explains the reasoning behind procedures contributes significantly to better retention rates. This approach emphasizes that while screening personnel can work at various locations, the training philosophy, certification/qualification methods, and supervision practices can set an organization apart and improve

⁵⁰ Chavallaz, Alain, Adrian Schwaninger, Stefan Michel, and Juergen Sauer. “Work Design for Airport Security Officers: Effects of Rest Break Schedules and Adaptable Automation.” *Applied Ergonomics* 79 (2019): 66–75.

staff retention. Understanding the “why” behind requirements rather than just procedural compliance helps create more engaged and committed screening personnel.

10.2 Recommendations and Implementation Guidance

1. EVALUATE STAFFING MODEL OPTIONS BASED ON AIRPORT-SPECIFIC FACTORS

Conduct a comprehensive assessment of direct employee, contractor, and hybrid staffing models to determine the most appropriate approach for your airport’s specific operational context, governance model, culture, risk profile, and constraints.

Implementation Guidance: Begin by evaluating your airport’s governance structure, available resources, operational requirements, and labor market conditions to determine the most suitable staffing approach. Consider these key factors for each model:

- **Direct Employee Model:** Assess your ability to manage higher personnel costs including benefits and equipment, handle staffing coverage during absences, and integrate screening staff with broader security operations. This model provides increased control over quality and performance but requires significant administrative infrastructure and may face lengthy hiring processes.
- **Security Contractor Model:** Evaluate not only the availability and experience of qualified security vendors in your market, but also their demonstrated ability to recruit, retain, and manage personnel who are both willing to commit to the demands of the job. Consider your airport’s capacity for contract oversight and quality control, as well as your tolerance for potential turnover issues. This approach offers faster implementation and staffing flexibility, but requires robust contract management, dedicated airport compliance staff, and effective oversight mechanisms.
- **Hybrid Model:** Determine which positions require higher levels of responsibility and knowledge versus those that can be effectively contracted. One airport found success using direct employees for supervisory and specialized roles while contracting for routine monitoring positions, though this requires managing two different workforce types.

2. ESTABLISH ROBUST SECURITY SERVICES CONTRACTS

Develop comprehensive security services contracts with clear performance standards, enforcement mechanisms, and aviation-specific requirements to ensure effective contractor management.

Implementation Guidance: Verify whether existing municipal or authority-wide contracts can be leveraged but ensure they include aviation-specific performance standards and training requirements. When developing security services contracts, consider incorporating specific performance metrics and enforcement mechanisms, including financial penalties for non-compliance with graduated fines based on violation severity and frequency. Define clear violations such as unauthorized phone use on post, unprofessional conduct, late reporting, failure to remove an employee upon the airport’s request, or incomplete documentation. Structure contracts to maintain airport control over training standards, uniform requirements, and performance metrics, ensuring you have the tools needed to enforce compliance and maintain security standards. Design solicitations to encourage competitive bidding and broader vendor response to ensure best value. Build flexibility to accommodate changing requirements and screening volumes without excessive change order costs. Consider requiring contractors to maintain specific staffing levels of trained personnel to ensure continuity despite turnover, and to have the capacity to provide surge staffing when operational needs demand.

3. IMPLEMENT DATA-DRIVEN STAFFING AND SCHEDULING

Establish processes to analyze employee traffic patterns and develop scheduling approaches that optimize staffing levels while managing costs.

Implementation Guidance: Utilize badge access control data to understand peak arrival times, traffic volumes, and employee movement patterns. Align security staff scheduling with actual employee shift patterns. Consider opening screening checkpoints 30 minutes before the start of passenger screening and major shift changes and align staff scheduling with employee shift patterns. Implement flexible staffing that allows multiple screening lanes to open during peak periods while consolidating to fewer lanes during slower times. Develop business continuity plans addressing staffing needs during emergencies, including arrangements for temporary housing, transportation, and shift coverage during weather events or other disruptions.

4. ADDRESS RETENTION CHALLENGES PROACTIVELY

Develop comprehensive strategies to attract and retain qualified screening personnel in a competitive labor market.

Implementation Guidance: To address retention challenges, prioritize fostering a positive work environment and offer competitive compensation and benefits that recognize employees' performance and their contributions to security. Recognition and reward programs for exceptional performance support employee retention and morale. Consider implementing job rotation programs to expand skills and reduce burnout. If using contractors, build strong partnerships by treating contract personnel as extensions of your security team. Fostering a supportive environment where staff feel safe to learn from mistakes without fear of blame can enhance workforce satisfaction and retention across all staffing models, whether direct employees, contractors, or a hybrid approach. Consider that effective quality training focusing on the "why" behind procedures, not just compliance, can be a key retention tool.

SECTION 10 QUICK REFERENCE

- Evaluate staffing models (direct, contractor, hybrid) based on your airport's specific factors, i.e., operational context, governance model, culture, risk profile, and constraints
- Use data-driven approaches to determine appropriate staffing and scheduling of screener personnel
- Address retention challenges with comprehensive strategies to attract and retain employees

SECTION 11: TRAINING AND QUALITY ASSURANCE

Training and quality assurance systems determine whether screening personnel can maintain the competency and consistency required for effective threat detection. Employee screening presents unique workforce development challenges that demand tailored approaches to both skill-building and performance monitoring. This section examines how airports design and implement training and quality assurance systems for employee screening operations, including initial and recurrent training approaches, quality control mechanisms, and performance evaluation systems.

11.1 Building Competency and Maintaining Effectiveness

Screening personnel face unique challenges when processing colleagues, authority figures, and familiar individuals through checkpoints multiple times daily. While employees are more predictable in the items they bring, this predictability increases the risk of familiarity-based security lapses and heightened vulnerability to insider threats. Research participants noted that employee pushback presents a particular challenge when programs are first established, with some employees testing limits and sometimes being disrespectful to screeners. The repetitive nature of screening tasks compounds these challenges, as complacency can develop over time without targeted mitigation strategies. Quality assurance should aim to achieve both operational practicality and efficacy, ensuring strong performance without imposing excessive testing demands that could negatively affect workforce morale.

11.1.1 Initial Training Programs

Initial training duration varied significantly across programs, reflecting differences in technology complexity and operational requirements. One airport implementing advanced technology noted that contractors initially struggled with the complexity, requiring a dedicated training environment before opening operational portals. Multiple airports structured their training programs with a comprehensive orientation followed by specialized technical training managed by security contractors.

The content of initial training programs typically includes several key components:

- **Equipment operation and technical procedures:** Training on x-ray machines, metal detectors, ETD equipment, and other screening technologies
- **Prohibited items recognition:** Comprehensive understanding of weapons, explosives, incendiaries, and other items not permitted in secure areas
- **Screening techniques:** Proper procedures for physical searches, bag inspections, and alarm resolution
- **Documentation requirements:** Record-keeping responsibilities and proper documentation of incidents
- **Regulatory knowledge:** Understanding of TSA requirements, provisions, and legal considerations
- **Customer service skills:** Professional interaction with employees being screened, including conflict de-escalation techniques

Three airports emphasized incorporating training that equips personnel with strategies for dealing effectively with challenging or difficult individuals. This includes teaching screeners techniques for managing tense interactions, de-escalating conflicts, and maintaining professionalism when faced with employees who may be frustrated, uncooperative, or high-ranking. Research participants identified

employee resistance as a notable challenge, with some staff members pushing boundaries and showing disrespect toward screeners, which necessitates targeted training to manage these behaviors.

Some organizations have found that focusing on quality training that explains the reasoning behind procedures, combined with strong supervision, improves both performance and retention. Understanding the “why” behind requirements rather than just procedural compliance helps create more engaged and committed screening personnel.

Several interviewed airports highlighted scenario-based training as particularly valuable, using real-life experiences from their own and other airports’ operations. These scenarios include handling situations when individuals present law enforcement credentials without proper airport badges, managing screening of high-ranking officials who may expect preferential treatment, and addressing conflicts when familiar employees become upset about screening requirements.

11.1.2 Recurrent Training Requirements

The majority of airports involved in the study conduct recurrent training either semi-annually or annually, while four airports hold quarterly refresher sessions for specific skills such as x-ray image interpretation. Several organizations reported implementing more frequent recurrent training, with face-to-face delivery considered essential for effectiveness. Airports consistently emphasized that maintaining currency through regular training is more effective than lengthy initial training alone.

Several airports highlighted complacency as a key challenge requiring targeted training interventions. Approaches include regular rotation of personnel between different posts, knowledge-based check-ins during shifts, and scenario-based exercises focusing on detection of less common threats. Two airports reported using technology-based solutions where screening personnel answer questions about procedures during their shifts, building what one airport described as “muscle memory” for critical tasks.

11.1.3 Training Development and Cross-Training Programs

Training plays an important role in both recruitment and retention of screening personnel. Airports involved in this study highlighted the value of comprehensive initial training, continuous development opportunities to keep staff engaged, and ensuring training bridges the gap between classroom learning and operational realities. One international airport emphasized the importance of addressing the disconnect between theoretical knowledge and real-world situations, recommending incorporation of practical scenario training.

Cross-training programs can prepare screening staff to perform various security duties beyond employee screening, particularly under the direct airport employee and hybrid models described in *Section 10.1*. These programs enable personnel to conduct AOA gate vehicle inspections, terminal and perimeter security patrols, Sterile Area monitoring, regulatory compliance activities, surveillance and deterrence functions, construction site security, emergency response staging, and special events security support. This approach provides operational flexibility during slower screening periods while reducing monotony and increasing job satisfaction through varied responsibilities. Additionally, cross-trained personnel can perform traffic management at terminals, visitor access control at office buildings, cargo and hangar area patrols, and critical infrastructure site monitoring.

Two airports in the research pointed out that finding staff who are willing and able to learn about new technologies is crucial. Legacy personnel with many years of experience at the airport may struggle to adapt to updated systems and procedures. This challenge has become an important factor in hiring,

allocating, and retaining staff, as it directly impacts the effectiveness of technology-driven screening operations.

11.1.4 Quality Control and Testing Programs

Quality control approaches varied significantly across airports in the research, although most emphasized multi-layered oversight systems combined with structured testing programs. Effective quality control requires both an organizational framework for oversight and systematic testing methods to assess screening effectiveness.

MULTI-TIERED OVERSIGHT STRUCTURES

One major airport authority described a three-tiered quality assurance approach that provides comprehensive oversight from multiple perspectives:

- **Tier 1: Security Contractor Level** – At the security contractor level (where applicable), dedicated quality assurance teams from contractor headquarters conduct independent testing alongside local supervisors and management. Contractors may deploy QA teams that review multiple checkpoint locations, providing consistency assessments across the operation.
- **Tier 2: Local Airport Level** – At the local airport level, security management or dedicated compliance teams conduct independent oversight focused on areas showing increased non-compliance as well as proactive assessments of other compliance areas. This tier provides direct airport control over quality standards regardless of staffing model.
- **Tier 3: Authority/Enterprise Level** – At the authority or enterprise level (for multi-airport operators), central office inspection teams conduct assessments across all facilities, enabling cross-facility comparison and identification of system-wide trends.

While this three-tiered structure represents a comprehensive model, most airports in our research implemented simpler two-tier systems combining contractor oversight with airport-level quality assurance. The appropriate structure depends on organizational complexity, staffing model, and available resources.

TESTING PROGRAM COMPONENTS

Testing programs emerged as a key quality control mechanism across the airports studied, typically incorporating both covert and overt testing approaches that serve distinct assessment purposes.

- **Covert Testing:** Methods reported include planting test articles to assess detection rates, using volunteers from other airport departments as test subjects to avoid recognition, and conducting unannounced inspections by quality assurance teams. Varying test articles and scenarios helps prevent predictability and provides more accurate assessment of actual screening capabilities. One international airport specifically targets testing of airport authority figure screening due to higher failure rates observed in this area.
- **Overt Testing:** This approach complements covert methods by evaluating screeners' demonstrated knowledge and procedural compliance under direct observation. One airport developed structured competency assessment forms that evaluate screening personnel across three dimensions: knowledge of policies and procedures, communication skills when interacting with aviation workers, and practical alarm resolution abilities. These standardized QA forms cover five core screening functions: two-factor authentication, personnel screening, personal property screening, ETD screening, and TSA checkpoint escort procedures. The forms include specific competency items assessed with checkboxes, enabling consistent evaluation across all screeners. Sample QA forms demonstrating this approach are provided in *Appendix A*.

TESTING FREQUENCY AND CADENCES

Testing frequency varied across airports in the research based on program size and operational complexity. Multiple airports conduct quarterly testing programs to maintain baseline oversight. One international airport reported conducting a minimum of eight inspections annually (often 11–15), two formal audits every two years, and three covert tests monthly. One hub airport reported conducting 500–600 competency tests monthly to maintain standards across a large-scale operation, up from 200–300 previously.

Airports operating multiple employee screening checkpoints or processing high volumes of personnel may benefit from more frequent testing cadences. The appropriate frequency depends on factors including program maturity, identified deficiency trends, and available quality assurance resources.

TECHNOLOGY-ENABLED QUALITY ASSURANCE

CCTV systems have become integral to quality control programs, enabling remote monitoring of screening operations without disrupting workflow. Several airports in the research utilize camera footage for quarterly audits of contractor performance, reviewing recordings alongside training files and conducting in-person observations as part of comprehensive oversight programs. Camera systems support multiple quality assurance functions including real-time supervision of screening procedures, documentation of proper technique application, and identification of training needs based on observed performance gaps. One airport reported using recordings to conduct “mock TSA inspections” by their compliance teams, reviewing footage to ensure procedures meet regulatory standards before actual TSA assessments.

Audio-enabled CCTV systems provide additional quality assurance value by capturing verbal instructions, clarifying disputed interactions, and providing more complete documentation when investigating complaints or security violations. Additionally, two airports equipped screening personnel with body-worn cameras to ensure audio capture of screening interactions, particularly where fixed CCTV systems lack audio recording capability or where ambient noise limits audio quality. One of these airports conducts periodic supervisory audits of body camera footage as part of its quality assurance program.

PERFORMANCE INCENTIVES

One airport operates an incentive program written into contractor agreements where guards can earn up to \$400 extra per quarter based on performance criteria from quality audits. This approach ties compensation directly to quality assurance results, creating financial motivation for maintaining high performance standards.

11.1.5 Performance Metrics and KPI Development

Among the airports interviewed, performance evaluation systems track various metrics to assess screening effectiveness and efficiency. Effective key performance indicator (KPI) programs connect specific metrics to program objectives, enable both individual and program-level assessment, and generate data that drives actionable improvement decisions.

CORE PERFORMANCE METRIC CATEGORIES

Airports in our study reported tracking metrics across several categories:

- **Throughput Rates:** Tracking the number of employees screened per hour or per day helps assess operational efficiency. Some airports measure as a simple count, while others segment data by checkpoint location, organization, or time period (such as peak hours versus off-peak).

One airport models this data to inform staffing decisions and adjust personnel deployment based on portal usage patterns.

- **Alarm Rates:** Tracking the frequency of alarms triggered during screening can indicate either effective threat detection or excessive false alarms requiring equipment adjustment. Monitoring both total alarms and resolution outcomes helps distinguish equipment sensitivity issues from actual security concerns.
- **Prohibited Item Detection:** Tracking the number and types of prohibited items identified provides insight into screening effectiveness. Some airports capture additional data elements including item type (weapons, tools, other prohibited items), detection method (x-ray, WTMD, ETD, pat-down, voluntary disclosure), and location where the item was found (on person, in bag, in specific pocket or compartment). Categorizing items enables trend analysis and targeted training interventions.
- **Procedural Compliance:** Measuring adherence to established screening protocols and documentation requirements helps identify inconsistent application of procedures. One organization reported monthly measurement of strict KPIs including procedural incident responsiveness and SOP compliance, enabling rapid identification of procedural drift.
- **Customer Service:** Capturing feedback from screened employees regarding professionalism and courtesy provides insight into stakeholder experience. One organization assesses whether employees felt they were treated appropriately and with courtesy through regular surveys. This practice, while uncommon among domestic airports in our research, provides valuable feedback for maintaining positive stakeholder relationships.

MEASURING DETECTION EFFECTIVENESS

Beyond tracking what screening programs detect, understanding what is missed provides actionable intelligence for improvement. Detection rate analysis combines results from covert testing, image interpretation assessments, and observational reviews to create a more complete picture of screening proficiency.

A detection rate can be calculated by comparing items successfully detected against total items tested during covert assessments: $\text{Detection Rate} = (\text{Items Detected} \div \text{Items Tested}) \times 100$. Tracking this metric at both individual screener and program levels enables targeted interventions where performance gaps exist.

Analyzing characteristics of missed items can reveal patterns requiring attention. Data elements some airports track include:

- **Item type:** What categories of items are most frequently missed during testing
- **Concealment location:** Where missed items were hidden (pockets, bags, lunch containers)
- **Detection method gaps:** Which screening method failed to identify the item
- **Circumstantial factors:** Time of day, checkpoint traffic volume, or other conditions present during misses

This analysis helps identify whether misses result from equipment limitations, procedural gaps, or training deficiencies, enabling appropriate corrective action.

INDIVIDUAL PERFORMANCE TRACKING

Systems that track individual screener performance enable targeted coaching and support. Where technology systems require individual logins, performance data can be associated with specific

personnel. This capability supports identification of high performers for recognition as well as individuals requiring additional training or supervision.

11.1.6 Continuous Improvement Practices

Most airports surveyed have implemented practices for incorporating lessons learned from testing, evaluations, and operational experience into their training and procedures. These improvement practices help programs adapt to emerging challenges and maintain effectiveness over time.

INCORPORATING TESTING RESULTS

Common approaches include incident-based testing adjustments, where testing focus shifts based on observed trends such as increased weapons discoveries or patterns in missed items. When testing reveals specific detection gaps, training can be adjusted to address those areas. For example, if covert testing shows frequent misses of items in particular locations or of certain types, targeted training exercises can reinforce detection of those specific scenarios. Airports also reported implementing immediate training updates when procedures change, ensuring personnel receive timely instruction on new or modified protocols.

Periodic conduct violation trend analyses, such as those performed every six months, are used to identify patterns and determine whether corrective actions have led to improvement. This systematic review of accumulated data helps distinguish isolated incidents from systemic issues requiring broader intervention.

ENGAGING SCREENING PERSONNEL

Involving screening personnel in evaluating new equipment, procedures, and training programs can provide valuable input on whether changes will enhance operations or create unnecessary complexity. One airport implementing a new screening technology reported conducting quarterly meetings with screening staff to gather feedback and answer questions, using this input to make procedural adjustments that improve both effectiveness and practicality. Establishing regular channels for screening personnel to share insights and propose enhancements based on their operational experience supports ongoing program refinement.

Two airports emphasized the importance of positive reinforcement alongside deficiencies. Rather than focusing solely on failures, these airports demonstrate proper techniques and explain the reasoning behind procedures, using what one described as an “amiable approach through conversation” to enhance understanding and encourage continued strong performance.

EXTERNAL BENCHMARKING

Partnerships with other airports to share best practices and learn from their experiences provide valuable external perspective. This approach can provide tested solutions to common challenges and identify improvement opportunities that internal review might overlook.

11.2 Recommendations and Implementation Guidance

1. ESTABLISH STRUCTURED INITIAL TRAINING PROGRAMS

Develop comprehensive initial training that combines technical skills with strategies for dealing effectively with challenging individuals to prepare screening personnel for the unique challenges of employee screening.

Implementation Guidance: Design training programs of appropriate duration based on screening complexity and operational needs. Include scenario-based exercises drawn from actual incidents at your

and other airports, particularly focusing on challenging situations like screening authority figures or handling upset employees. Incorporate training that equips personnel with strategies for managing tense interactions, de-escalating conflicts, and maintaining professionalism when faced with employees who may be frustrated, uncooperative, or high-ranking. Focus training on explaining the reasoning behind procedures, not just compliance, as several participants report this approach significantly improves both performance and retention.

2. IMPLEMENT REGULAR RECURRENT TRAINING PROGRAMS

Establish ongoing training requirements that maintain competency and combat complacency through regular skill reinforcement and knowledge updates.

Implementation Guidance: Schedule recurrent training annually, semi-annually, or quarterly based on operational needs and complexity. High-volume operations may benefit from more frequent training sessions, allowing focus on areas of concern and SOP changes. Focus recurrent training on addressing identified weaknesses from quality control testing, incorporating lessons learned from incidents, and introducing updates to procedures or equipment. This process facilitates continuous improvement and reinforces the effectiveness of training and quality assurance measures. Consider implementing technology-based daily knowledge reinforcement, where screeners answer procedural questions during shifts to maintain awareness. Address complacency and knowledge gaps through varied training approaches including role-playing exercises, surprise scenario injections, and cross-training on different screening positions. Prioritize face-to-face training delivery over e-learning when possible, as multiple organizations reported better outcomes with in-person instruction.

3. DEVELOP CROSS-TRAINING PROGRAMS FOR OPERATIONAL FLEXIBILITY

Implement training programs that enable screening personnel to perform multiple security functions, maximizing workforce value and operational flexibility, particularly for airports using direct airport employee or hybrid staffing models.

Implementation Guidance: For airports employing direct airport security personnel or hybrid models combining direct employees with contractors, develop cross-training curricula that prepare screening staff to perform various security duties beyond employee screening. The airports in the study that successfully implemented cross-training programs relied on direct airport employees who could be assigned to a variety of security functions. These roles included:

- Traffic monitoring and regulation
- Parking enforcement
- Merchandise and vendor inspections
- Random vehicle inspections on the airfield
- Random ID media checks
- Other security-related duties

This approach offers several benefits, such as improved staff utilization during slower screening periods, reduced monotony and increased job satisfaction, enhanced understanding of overall security operations, and greater scheduling flexibility.

Note that cross-training programs are most feasible with direct employees due to the airport's control over job descriptions, training requirements, and deployment flexibility. Airports using contractor-only models may face limitations in implementing cross-training due to contractual constraints and the specialized nature of contracted services.

4. DEVELOP MULTI-TIERED QUALITY CONTROL SYSTEMS

Create layered oversight mechanisms with systematic testing programs to evaluate screening effectiveness from multiple perspectives.

Implementation Guidance: Establish quality control systems with at least two tiers of oversight appropriate to your organizational structure and staffing model.

- **Establish Contractor-Level Oversight:** Require security contractors to maintain their own quality assurance programs with regular testing and performance monitoring. Consider requiring vendor QA teams that conduct reviews across multiple checkpoint locations to ensure consistency. Supplement contractor oversight with dedicated security managers who are direct employees, providing independent on-site assessment. Embedding performance incentives directly into contractor agreements can strengthen accountability for quality outcomes.
- **Implement Airport-Level Oversight:** Conduct independent oversight through security management or dedicated compliance teams. Implement structured testing programs that include both covert and overt components serving complementary assessment purposes.
- **Design Covert Testing Programs:** Plant test articles using varied items and scenarios to prevent predictability. Enlist volunteers from other airport departments to serve as test subjects, maintaining test integrity by avoiding recognition. Specifically target testing of authority figure screening, where research indicates higher failure rates are common. Document all covert test results to enable trend analysis.
- **Design Overt Testing Programs:** Develop standardized competency assessment forms that evaluate screeners across knowledge, communication, and practical skills dimensions. Airports seeking to develop structured assessment tools may refer to *Appendix A*, which provides sample QA forms covering five core screening functions. Consider implementing “mock TSA inspections” by compliance teams to ensure readiness for regulatory oversight.
- **Establish Testing Cadences:** At minimum, quarterly testing provides baseline oversight for most programs. Airports operating multiple employee screening checkpoints or processing high volumes may benefit from monthly or more frequent testing. Select frequencies based on program maturity, identified trends, and available resources.
- **Leverage Technology for Remote Monitoring:** Use CCTV systems to provide both real-time oversight capability and recorded footage for periodic review. Camera coverage of screening operations supports quality assurance without disrupting workflow.

5. ESTABLISH PERFORMANCE METRICS AND KPI PROGRAMS

Develop structured programs for tracking performance metrics that connect to program objectives and provide actionable data for assessment and improvement.

Implementation Guidance:

- **Define Core Performance Metrics:** Identify specific metrics aligned with security objectives across multiple categories, typically including throughput rates, alarm rates, prohibited items detection, procedural compliance, and customer service feedback. Determine how each metric will be measured, at what frequency, and how data will be aggregated (by checkpoint, by organization, by time period, or program-wide).
- **Track Prohibited Item Detection Data:** Consider tracking data elements that enable detailed analysis: item type, detection method (x-ray, walk-through, ETD, pat-down, voluntary disclosure), and location where items were found. This granularity supports identification of patterns and targeted improvement efforts.

- **Implement Detection Rate Analysis:** Track both successful detections and misses identified through covert testing. Calculate detection rates by comparing items detected against items tested, tracking at both individual screener and program levels where feasible. Analyze characteristics of missed items to identify whether gaps stem from equipment limitations, procedural issues, or training needs. Understanding not only what is caught but what is missed, and the characteristics of those misses, provides powerful data for focusing improvement efforts.
- **Enable Individual Performance Tracking:** Where technology systems support individual logins, implement tracking that associates performance data with specific personnel. This enables targeted coaching for individuals showing performance gaps and recognition for high performers.
- **Conduct Regular Evaluations:** Combine quantitative metrics with qualitative assessments such as direct observation and competency demonstrations. Annual recertification requirements can validate continued proficiency across core screening functions.
- **Develop Feedback Mechanisms:** Create processes that both identify deficiencies and acknowledge good performance. When sharing testing results with personnel, demonstrate proper techniques and explain the reasoning behind procedures rather than simply highlighting failures. Consider implementing employee feedback surveys to assess customer service dimensions, gathering input on whether screened employees felt treated appropriately and courteously.

6. CREATE CONTINUOUS IMPROVEMENT MECHANISMS

Develop systematic practices for incorporating operational experience, testing results, and lessons learned into training and quality assurance programs.

Implementation Guidance:

- **Establish Review Cycles:** Create formal review cycles for training content and quality control procedures, with most airports in the research conducting reviews at least annually. Schedule periodic analysis of accumulated data, such as violation trend reviews every six months, to identify patterns and assess whether previous corrective actions have produced improvement.
- **Use Testing Data to Drive Priorities:** When covert testing reveals specific detection gaps, such as frequent misses of particular item types or concealment locations, develop targeted training exercises addressing those scenarios. Adjust testing focus areas based on emerging trends, shifting emphasis when patterns such as increased weapons discoveries or new concealment methods emerge.
- **Update Training Promptly:** Implement immediate training updates when procedures or equipment changes, ensuring personnel receive timely instruction on new or modified protocols. Avoid allowing gaps between procedural changes and corresponding training that could create confusion or inconsistent application.
- **Engage Screening Personnel:** Establish channels for screening personnel to share operational insights and propose enhancements based on their experience. Consider regular meetings (such as quarterly) where staff can provide feedback on procedures, equipment, and training effectiveness. Actively involve personnel in evaluating proposed changes to assess whether modifications would enhance operations or create unnecessary complexity.
- **Consider External Partnerships:** Establish partnerships with other airports implementing full employee screening programs to share best practices and learn from their experiences. External perspectives can identify improvement opportunities that internal review might overlook.

- **Balance Feedback Approaches:** Recognize strong performance alongside correcting weaknesses to maintain workforce morale and encourage continued excellence.

SECTION 11 QUICK REFERENCE

- Develop and maintain effective training and quality assurance measures to ensure compliance with regulatory and airport requirements, strengthen risk mitigation, and enhance the efficacy of a full employee screening program.
- Implement regular recurrent training to maintain competency, decrease knowledge gaps, and combat complacency
- Develop multi-tiered quality control systems with structured testing cadences and both covert and overt testing components
- Ensure full CCTV coverage of screening operations, including personal property inspection areas, and consider audio recording capability to support quality assurance and complaint resolution
- Establish KPI programs tracking throughput, detection, compliance, and customer service metrics with sufficient detail to enable trend analysis and targeted improvements
- Implement detection rate analysis to understand both what is detected and what is missed, using findings to focus training and procedural refinements
- Create continuous improvement practices incorporating lessons learned from testing, trend analysis, and frontline personnel feedback
- *Appendix A* provides sample QA forms for structured screener competency assessments

SECTION 12: REGULATORY CONSIDERATIONS

Implementing full employee screening programs requires airports to address both regulatory frameworks and legal requirements. These interconnected considerations, which range from federal TSA requirements to constitutional protections and workplace accommodation obligations, establish the boundaries within which screening operations must function, and significantly influence program design decisions.

12.1 Regulatory Framework and ASP Integration

The regulatory landscape for full employee screening continues to evolve as TSA responds to identified insider threats and emerging security concerns. While TSA does not currently mandate full employee screening, airports may choose to implement more robust screening programs based on their risk assessment, alignment with international standards, or strategic security considerations. How an airport's full employee screening program fits within the regulatory framework has important implications, and airports have approached this in a number of different ways.

Federal regulations issued by TSA under 49 CFR § 1542 provide the primary legal framework for airport security requirements. These regulations establish the foundation for ASP requirements, screening and vetting mandates, and other security measures that airports must implement.

Airports implementing full employee screening face a fundamental strategic decision: how to integrate their programs with ASP documentation and federal regulatory requirements. The documentation strategy selected shapes how airports coordinate with TSA and how easily programs can be modified, scaled, or adapted to changing operational needs without triggering the formal process for amending an ASP.

12.1.1 ASP Content and Amendment Process

Each commercial service airport operator is required to implement an ASP that must be approved by TSA prior to the start of commercial operations, as outlined in 49 CFR § 1542. The ASP must clearly identify the boundaries and requirements for each security area (Secured Area, Sterile Area, AOA, and SIDA), the airport's access control and badging systems, law enforcement support, training, and incident response procedures. Full employee screening should be viewed as one layer within an airport's broader security approach, complementing rather than replacing the other required security measures.

How airports integrate their full employee screening programs into their ASPs varies considerably, with three distinct documentation strategies emerging from the research:

STRATEGY 1: COMPLETE SEPARATION

Three airports in the study have successfully operated comprehensive screening programs entirely outside their ASP framework. This approach treats full employee screening as an operational enhancement beyond regulatory requirements, maintaining all procedures in separate SOPs while including only mandatory AWS compliance language in the ASP.

Benefits of this approach include maximum operational flexibility (procedures can be modified without TSA approval), reduced regulatory burden (voluntary measures not subject to TSA inspection findings), and simplified scaling based on operational needs. Multiple airports in the research emphasized that this strategy "prevents over-regulation and findings resulting from security measures that are not required." However, this approach may not be feasible when TSA coordination for alarm resolution necessitates

formal procedures, local FSD interpretation requires inclusion, or when an international agreement, such as One-Stop Security, requires ASP documentation of the airport's full employee screening program (see ICAO Standards and International Agreements below for detailed discussion).

STRATEGY 2: MINIMAL DOCUMENTATION

The majority of airports in this study keep ASP language “minimal but sufficient,” ensuring that future calibrations or expansions of their employee screening program will not require rewriting the ASP. This approach includes only high-level program information, such as program existence, the number of screening checkpoints, and their locations. Detailed procedures are maintained by the airport in separate SOPs. This approach provides flexibility to adjust procedures as needed without requiring TSA approval for every operational or procedural change.

STRATEGY 3: INTEGRATED DOCUMENTATION

A smaller number of airports incorporated more detailed screening procedures into their ASPs. This approach may be necessary for airports that rely on TSA checkpoints for alarm resolution, as they may need to document chain-of-custody procedures for employees with unresolved alarms. One airport worked extensively with TSA to document these protocols in their ASP, describing this as their “biggest hurdle.” Additionally, airports with international One-Stop Security agreements may be required to include detailed procedures in their ASPs for inspection by foreign authorities (see ICAO Standards and International Agreements below for detailed discussion). *For detailed discussion of how these ASP decisions affect operational procedures and SOP development, see Section 9.1.*

The ASP amendment process itself typically follows five key stages: (1) initial communication between TSA and the airport, (2) verbal agreement on amendment language and intent, (3) airport sends draft version to TSA, (4) TSA comments are incorporated, and (5) draft amendment is submitted for final approval. Some airports in the research have found success using temporary amendments during the initial implementation of employee screening, which allowed for adjustments while establishing the program before filing a permanent ASP change. The temporary amendment also reduced the administrative burden for the airport and TSA during early stages of implementing their full employee program.

However, multiple airports in our study reported inconsistent ASP requirements and interpretations across different airports and FSDs. One airport noted challenges with ASP requirements that were not consistent with nearby airports in the region, highlighting the variability in how TSA field offices approach ASP amendments for employee screening.

A number of airports stressed the importance of early and frequent engagement with TSA during the planning and implementation of employee screening programs. One airport explained they worked closely and maintained regular coordination with TSA regulatory staff throughout the development process. Some airports reported success with collaborative approaches to TSA coordination, with one noting that close coordination with TSA and pre-approval of draft language for its ASP amendment streamlined the approval process. However, airports also reported challenges in coordination with TSA, particularly regarding interpretation of requirements, with one airport noting challenges with unclear TSA guidance and confusion between ASP allowances and local FSD directions.

12.1.2 TSA Coordination for Alarm Resolution

Airports relying on TSA checkpoints for alarm resolution may need additional ASP documentation. One airport worked extensively with TSA to document chain-of-custody procedures in their ASP, describing this as their “biggest hurdle.” The documented protocol specifies: employee alarms during screening → screening personnel unable to resolve alarm using divestiture and handheld metal detector → airport

police escort employee to TSA checkpoint → TSA assumes responsibility and attempts to resolve the alarm.

However, this approach requires local FSD agreement. One airport initially planned to avoid conducting pat-downs through TSA referral but was forced to implement pat-down procedures when the FSD denied their checkpoint escort option. This airport subsequently added their SOP as an appendix to their ASP, which allows them to update operational procedures more easily without needing to undergo the formal ASP amendment process. This variability in TSA FSD interpretations and practices makes early coordination essential for airports planning this approach.

12.1.3 TSA AWS Requirements

Regardless of which ASP documentation strategy airports choose for their full employee screening programs, all must address TSA's baseline screening requirements. In 2023, TSA issued the AWS NA, which introduced new requirements for screening aviation workers with unescorted access to a Secured Area or Sterile Area from a public area in a passenger terminal building. The amendment mandates signage, notification procedures, and penalties for noncompliance, and requires airports to conduct random continuous screening at designated access points. TSA also developed various tools and resources to support airports in implementing AWS requirements. The Random Screening Scheduler tool helped airports calculate required screening hours and generate randomized schedules to ensure unpredictability in screening operations. This regulatory shift reflects TSA's growing concern about insider threats and the need to strengthen access control measures, although it stops short of requiring 100% employee screening.

RELATIONSHIP BETWEEN FULL EMPLOYEE SCREENING AND AWS REQUIREMENTS

Airports implementing full employee screening at dedicated checkpoints must understand that this *does not* eliminate the requirement to conduct AWS random screening at other access points. Full employee screening enhances security at primary entry points but must be complemented by random AWS screening operations at other direct access points where full screening is not implemented.

RECENT LEGAL DEVELOPMENTS: CITY OF BILLINGS V. TSA

In August 2025, the US Court of Appeals for the DC Circuit vacated TSA's AWS NA in *City of Billings v. TSA*,⁵¹ ruling that TSA failed to follow proper notice-and-comment procedures under the Administrative Procedure Act.⁵² The court noted that "TSA and Congress have grown increasingly concerned about the security risk posed by airport workers with unescorted access to secured airport areas" and recognized these significant aviation security concerns.⁵³ While vacating the amendment due to procedural defects, the court withheld its mandate to allow TSA time to adopt a procedurally sound rule, requiring TSA to submit status reports every 60 days on its progress.⁵⁴ This recent legal development creates uncertainty about future federal mandates but does not affect airports that voluntarily implement full employee screening programs.

12.1.4 Compliance with Airport Security Rules and Regulations

In addition to federal regulations issued by TSA, many airports have established their own airport security rules and regulations. These are enacted either by airport authorities or by municipal, county, or state governments, and they govern employee behavior while also establishing the airport's authority to

⁵¹ *City of Billings v. TSA*, No. 24-1123, 2025 WL 3576892 (D.C. Cir. Aug. 15, 2025).

⁵² 5 U.S.C. § 553.

⁵³ *City of Billings*, 2025 WL 3576892, at *4.

⁵⁴ *Id.* at *12.

enforce security requirements.⁵⁵ These rules provide the foundation for enforcement mechanisms and accountability measures that support full employee screening programs.

Structured enforcement systems for regulatory violations discovered during employee screening formalize accountability. One airport uses a formal violation notice system with escalating fines for prohibited items violations, starting at \$250 for first offenses and increasing to \$500 for second offenses. Violation severity levels can also be calibrated based on the type and characteristics of prohibited items discovered, with factors such as blade length potentially affecting whether an item constitutes a policy violation or a criminal offense under applicable state weapons statutes. *For discussion of state law definitions and their application to prohibited item enforcement, see Section 13.1.1.* These violation notice systems often incorporate automated notification capabilities, with one major airport implementing automated emails to authorized signatories when their employees receive violations, ensuring immediate awareness and promoting organizational accountability for compliance.

Badge suspensions, revocations, and reduced badge renewal periods can also improve accountability for employees who attempt to bypass or withdraw from screening or are discovered with prohibited items. One airport reported that authorized signatories with the most security violations must conduct refresher training covering all violation categories with their employees, placing accountability on employers for their workers' compliance. This approach shifts responsibility to employers, badge sponsors, and vendors and creates incentives for companies to ensure their employees understand and follow screening requirements. Badge reinstatement procedures typically require completion of mandatory security training courses, with the reinstatement process occurring several days after all required training is completed. This creates a deterrent effect and ensures comprehensive retraining before access privileges are restored.

AIRPORT ENFORCEMENT TOOLS: A MULTI-LAYERED APPROACH TO PENALTIES

Effective enforcement relies on a clear, published penalty structure that ensures transparency and consistent application. In the full employee screening context, this structure addresses violations of airport security rules and regulations such as attempting to bypass or withdraw from screening and possession of prohibited items discovered during screening. Airports utilize a range of monetary and non-monetary penalties that can be applied to individual employees, their supervisors, and their employers to foster a broader culture of security accountability.⁵⁶ Penalties for individual badge holders often include:

- **ID Media Penalties:** These are highly effective non-monetary tools. They can range from temporary **badge suspension** for a set period (e.g., 7 to 30 days) to permanent **badge revocation** for the most serious offenses.⁵⁷ A suspension is particularly impactful as it often prevents the employee from working in secure areas, potentially leading to a loss of income.⁵⁸
- **Mandatory Retraining:** This is a common requirement following a violation and is often a prerequisite for the reinstatement of a suspended badge.⁵⁹

⁵⁵ Scott Houston et al., *Optimizing Compliance with Airport Security Rules and Regulations*, PARAS 0054 (Washington, DC: National Safe Skies Alliance, January 2025), 8.

⁵⁶ Ibid., 37–38.

⁵⁷ Ibid., 35.

⁵⁸ Ibid., 37.

⁵⁹ Ibid., 35.

- **Monetary Fines:** Airports with the legal authority to do so may issue fines directly to individuals. These fines can be part of a progressive fee structure that increases with the frequency and severity of violations.⁶⁰

Penalties for tenant companies and employers are designed to be significant enough that they cannot be dismissed as a mere “cost of doing business” and include:

- **Company-Level Fines:** For systemic or repeated violations by employees, airports may assess fines directly against the employer.⁶¹
- **Targeted ID Media Penalties:** Rather than penalizing a single employee, an airport may shorten the badge expiration and renewal periods for an entire company (e.g., from two years to one year or six months), increasing the administrative burden on the tenant to compel better oversight.⁶² In more severe cases, an airport may suspend the sponsoring company’s ability to sponsor new airport badges, directly impacting their ability to staff their operations.⁶³

THE ROLE OF TENANT LEASES AND CONTRACTOR AGREEMENTS

Tenant leases and contractor agreements are critical supplementary enforcement tools, but they do not typically serve in lieu of an airport’s formal fining process. The formal process, which requires notice and an opportunity to be heard, establishes the violation and the corresponding penalty. The lease or contract then serves as a powerful pre-agreed legal mechanism to ensure financial accountability and simplify the collection of those penalties. These agreements often include clauses that:

1. Require the tenant to reimburse the airport for any fines levied on the airport by federal agencies (like the TSA or FAA) due to the tenant’s negligence.⁶⁴
2. Hold the tenant financially responsible for the airport’s own penalties, allowing the airport to add the fine amount to the tenant’s rent or other charges.⁶⁵

This contractual language empowers the airport to enforce compliance and recover costs without needing to initiate separate legal proceedings, but it functions in support of—not as a replacement for—the airport’s primary, due process-based violation and penalty system.

12.1.5 ICAO Standards and International Agreements

Recent changes in ICAO standards and emerging international agreements are reshaping how airports approach employee screening and regulatory compliance. In Amendment 17 to ICAO Annex 17 (adopted late 2019; effective 30 March 2020), Standard 4.2.5 requires Contracting States to ensure that persons other than passengers—and the items they carry—are screened before entering security-restricted areas, and Standard 4.2.6 requires the use of screening methods capable of detecting explosives and explosive devices, applied continuously or unpredictably.⁶⁶ ICAO standards are binding unless a state files a notified difference; nonetheless, ICAO expects states to collaborate in securing uniformity in aviation security matters. In June 2020, TSA filed an official difference to this ICAO standard, notifying ICAO that the multiple layers of security measures used in the United States achieve

⁶⁰ Ibid., 45–46.

⁶¹ Ibid., 47.

⁶² Ibid., 20.

⁶³ Ibid., 39, 44.

⁶⁴ Ibid., 41–42.

⁶⁵ Ibid.

⁶⁶ International Civil Aviation Organization. *Annex 17 to the Convention on International Civil Aviation: Security—Safeguarding International Civil Aviation Against Acts of Unlawful Interference*. Amendment 17. (adopted 25 November 2019; effective 30 March 2020; applicable 30 July 2020), Standards 4.2.5–4.2.6.

the same intended outcome.⁶⁷ Multiple airports indicated that they anticipate TSA will eventually mandate full employee screening to align with ICAO standards, although most believe this requirement is still several years away.

The emergence of international One-Stop Security agreements has created additional regulatory considerations for some airports. TSA has begun implementing a Congressionally authorized One-Stop Security pilot program designed to simplify international travel.⁶⁸ This program allows passengers arriving from select foreign airports to be exempt from TSA rescreening upon arrival in the United States. An operational assessment of the program began in July 2025, involving two flights originating from London's Heathrow International Airport (LHR).⁶⁹ The pilot includes an American Airlines flight to DFW and a Delta Air Lines flight to ATL.⁷⁰ To implement this program, the foreign airports must have security standards that both states agree are equivalent to their own.⁷¹ TSA anticipates better security, reduced costs, and an improved passenger experience for those traveling from a One-Stop Security location.⁷²

One airport reported that their participation in the One-Stop pilot explicitly required including their full employee screening program in the ASP, with UK authorities wanting SOPs included so they can be inspected. Thus, the potential opportunity of participating in One-Stop Security may provide additional justification and support for US airports to implement a full employee screening program.

12.2 Recommendations and Implementation Guidance

1. DEVELOP STRATEGIC ASP INTEGRATION APPROACH

Select the appropriate ASP documentation strategy from the three approaches identified in the research: complete separation, minimal documentation, or integrated documentation.

Implementation Guidance: Choose your documentation strategy based on your specific circumstances.

- **Complete Separation:** For maximum regulatory and operational flexibility, consider maintaining complete separation between your full employee screening program and your ASP, documenting only mandatory AWS compliance in the ASP while keeping all operating procedures for full employee screening in separate SOPs. However, this approach may not be feasible if your airport requires TSA checkpoint referral for alarm resolution or seeks to participate in the One-Stop Security program in the future.
- **Minimal Documentation:** If complete separation is not feasible, maintain minimal ASP language that provides necessary compliance without limiting future flexibility. Include only high-level elements such as program existence, number and general locations of checkpoints, and reference to applicable requirements.
- **Integrated Documentation:** Airports seeking to participate in One-Stop Security may be required to include detailed screening procedures or SOPs in their ASP for inspection by foreign

⁶⁷ TSA. *Letter to the Secretary General of the International Civil Aviation Organization*. Washington, DC: March 2020. (Referenced in GAO-21-273, p. 8.)

⁶⁸ TSA, "'One Stop Security' Pilot Program Aims to Simplify International Travel," *Transportation Security Administration*, August 27, 2025, accessed October 2, 2025, <https://www.tsa.gov/news/press/releases/2025/08/27/one-stop-security-pilot-program-aims-simplify-international-travel>.

⁶⁹ Ibid.

⁷⁰ Ibid.

⁷¹ Ibid.

⁷² Ibid.

authorities. Similarly, airports that rely on TSA checkpoints for alarm resolution may be required by TSA to document detailed chain-of-custody and other screening procedures in their ASP.

Regardless of approach, work closely with your FSD early in planning to understand local expectations. Consider using temporary amendments during initial implementation. Maintain detailed procedures in separate SOPs whenever possible to preserve operational flexibility.

2. UNDERSTAND THE CRITICAL DISTINCTIONS BETWEEN FULL SCREENING AND AWS REQUIREMENTS

Recognize that implementing full employee screening at consolidated checkpoints does NOT eliminate requirements for random continuous AWS at other access points.

Implementation Guidance: Full employee screening complements but does not substitute for AWS requirements. Even with comprehensive screening at main employee checkpoints, airports must continue conducting random AWS screening at direct access points where full screening is not implemented. Ensure your program design accounts for both requirements and budget accordingly. Ensure AWS screening operations are documented separately to avoid confusion with full screening procedures.

3. DEVELOP CLEAR ENFORCEMENT AUTHORITY AND PROCEDURES

Establish structured enforcement strategies and mechanisms for noncompliance with employee screening policies or discovery of prohibited items.

Implementation Guidance: Airports that have established security rules and regulations that govern or apply to their full employee screening program should consider:

- Implementing a structured, transparent, and progressive penalty structure, such as a **tiered violation matrix** or a **point-based system**. For minor infractions, consider a “no-fault” or informal warning system, such as a “Counseling Violation,” which provides on-the-spot training and documentation without immediate punitive action for a first offense.³
- Developing a penalty structure that holds all relevant parties accountable:
 - For individuals: Use a mix of non-monetary penalties like mandatory retraining and badge suspension, which can be more effective than small fines.
 - For employers: Implement company-level penalties for systemic or repeated violations by their employees. This can include significant monetary fines, requiring the tenant to develop a formal corrective action plan, or suspending the company’s badging privileges.

SECTION 12 QUICK REFERENCE

- Determine strategic ASP integration approach:
 - Complete Separation – provides maximum flexibility
 - Minimal documentation – provides necessary compliance without limiting future flexibility
 - Integrated documentation – may be required for airports seeking to participate in One-Stop Security; may also be required for airports that rely on TSA passenger screening checkpoints for alarm resolution
- Understand full screening does NOT eliminate AWS requirements at other access points
- Establish dual documentation systems for TSA compliance and local enforcement
- Prepare for international agreement requirements if applicable
- Develop enforcement procedures with clear legal authority
- Monitor *City of Billings* impact and TSA rulemaking progress

SECTION 13: LEGAL CONSIDERATIONS

Establishing a legally defensible employee screening program requires airports to ground their authority in constitutional principles while implementing practical measures that protect against liability exposure, respect employee privacy, and accommodate individual needs. These legal dimensions significantly influence operational decisions, from screening technology selection to staffing models and alarm resolution procedures.

13.1 Understanding Legal Issues and Considerations for Full Employee Screening

Airports face distinct challenges in balancing security needs with individual rights and operational practicality when implementing full employee screening programs. The legal landscape for employee screening encompasses multiple jurisdictions and authorities, from federal constitutional protections to state laws and local ordinances. Understanding these legal dimensions early in the planning process enables airports to design programs that withstand legal scrutiny while achieving security objectives.

13.1.1 Legal Authority for Full Employee Screening

Airports implementing full employee screening must establish clear legal authority drawing from multiple sources. The foundation rests on constitutional principles and administrative search doctrine at the federal level, while state statutes and local ordinances often provide important supplementary authority for enforcement mechanisms and specific operational requirements.

CONSTITUTIONAL AND ADMINISTRATIVE SEARCH AUTHORITY

The legal foundation for airport employee screening rests primarily on the administrative search exception to Fourth Amendment requirements. The screening of airport employees accessing secure areas constitutes a “search” subject to Fourth Amendment protection. However, these searches fall within the well-established administrative search doctrine, specifically as part of the “special needs” exception recognized by courts. This exception applies where the government’s interest in public safety justifies routine searches not predicated upon individualized suspicion but rather upon broader public safety needs.

The constitutionality of administrative searches at airports relies on balancing legitimate governmental interest in maintaining aviation security against the reduced expectation of privacy that employees possess in security-sensitive airport areas. Courts consistently recognize airports as sensitive environments where heightened security measures are both expected and justified. Judicial precedent supports administrative searches of both passengers and employees, provided these searches remain reasonable in scope and execution. Similar constitutional standards apply to both passenger and employee screening, although employee searches involve additional practical considerations due to frequency and operational context.

Constitutional compliance requires screening practices to be carefully tailored to avoid unnecessary intrusiveness or arbitrary enforcement. Screening methods must maintain proportionality between security needs and the degree of intrusion on privacy and personal dignity. Airports must ensure that methods used—such as metal detectors, pat-downs, x-ray machines, and ETD—are justified by legitimate security objectives and applied uniformly and fairly. Screening procedures must be clearly defined, consistently applied, and proportionate to underlying security objectives to minimize potential claims of unreasonable or arbitrary enforcement.

STATE AND LOCAL LEGAL AUTHORITY

Beyond federal constitutional requirements, a number of airports cited state statutes and local ordinances as important to establishing their authority to conduct employee screening, particularly regarding enforcement of security rules. These state and local laws frequently provide airports with additional frameworks that authorize more strict enforcement of security rules through citation authority, establish specific definitions for prohibited items or dangerous weapons relevant to screening operations, and create administrative procedures for searching individuals and seizing property. These statutory and regulatory authorities complement federal requirements and often provide airports with clearer enforcement mechanisms, particularly for handling items that may be legal under local laws but prohibited in secure areas. Airports should work closely with legal counsel to identify applicable state and local authorities that can strengthen their legal framework for employee screening operations.

State law definitions have also been particularly important for prohibited items policies. State statutory definitions of weapons and dangerous items are often incorporated into prohibited items policies and airport security rules. One airport worked closely with its legal team to ensure its employee screening program complied with state law definitions of dangerous weapons, specifically incorporating these definitions into its security rules and regulations. Another airport developed a comprehensive prohibited item list using TSA's list as a foundation while adding state law weapon definitions and airport authority regulations, creating a composite approach that strengthened legal authority for enforcement. Another airport specified tactical knives based on state law definitions (5.5-inch blades or larger) to align with prosecutable standards under state criminal statutes.

Strategic alignment with state law definitions provides multiple benefits: clearer enforcement authority for items that may be legal to possess but prohibited in secure areas, stronger basis for criminal prosecution when weapons are discovered, and reduced ambiguity in determining what constitutes a prohibited weapon versus a tool of trade. Airports should work with legal counsel to identify relevant state statutes that can strengthen their prohibited items enforcement framework.

For operational implementation of prohibited item policies, see Section 8.1

BOUNDARY DEFINITIONS FOR SECURED AREAS AND ENFORCEMENT AUTHORITY

The description of a Secured Area boundary in an airport's ASP can significantly affect enforcement authority and, in some states, the criminal prosecution of employees who violate security policies. For instance, one airport in Texas strategically redefined its Secured Area boundary to begin at the *entrance* of its employee screening portals rather than at the access point door on the other side. This change was critical for ensuring that employees discovered with prohibited weapons during screening could be effectively prosecuted under state law.

Under Texas Penal Code § 46.03, a person commits a third-degree felony if they possess a firearm, location-restricted knife (blade over 5.5 inches), club, or other prohibited weapon “in or into a secured area of an airport.”⁷³ The airport had been advised by local prosecutors that its previous boundary definition—which placed the start of the Secured Area *after* the screening checkpoint—created a legal loophole. An employee discovered with a weapon during screening could argue they had not yet officially entered the Secured Area and thus could avoid prosecution under this statute.

By redefining the boundary in its ASP to include the screening portal itself, the airport closed this loophole. Now, any individual entering the portal with a firearm, location restricted knife, club, or other prohibited weapon is immediately within the Secured Area as defined by both the ASP and state law.

⁷³ Tex. Penal Code Ann. § 46.03 (West 2023).

This provides law enforcement and prosecutors with a clear basis for pursuing a felony charge under § 46.03.⁷⁴

This strategy of aligning an airport's ASP-defined boundaries with state law is a powerful tool. Airports in Texas, or in other states with similar statutes prohibiting weapons in airport Secured Areas, should consider this approach. However, it requires careful coordination with legal counsel, local law enforcement, prosecutors, and the local TSA FSD to ensure the revised Secured Area boundaries are properly documented and understood by all parties.

For ASP documentation requirements, see Section 12.1.

13.1.2 Liability Management and Risk Mitigation

Among the airports surveyed, liability concerns emerged as a primary factor shaping operational decisions about employee screening programs, particularly regarding physical contact during screening. Airports face potential liability exposure from physical searches, discrimination claims, violations of privacy, and allegations of inappropriate conduct during screening procedures. The sensitivity of pat-down procedures—involving physical contact with employees' bodies—represents the most significant liability concern identified by airports in this study. Airports have taken divergent approaches to managing these liability concerns, with some eliminating physical contact entirely through no-touch policies while others have developed detailed protocols for conducting limited pat-downs within carefully defined parameters designed to minimize exposure.

13.1.3 No-Touch Policies and TSA Referral

Airports have adopted varying approaches to physical searches based on liability considerations. Some programs have implemented “no-touch” policies that avoid pat-downs entirely, instead referring individuals with unresolved alarms to TSA checkpoints for additional screening. Other programs offer pat-downs as a voluntary option, allowing employees to choose between a pat-down conducted by screening personnel or referral to a TSA checkpoint for alarm resolution. One major airport initially included private screening rooms for conducting pat-downs but removed them and stopped conducting pat-downs entirely due to legal concerns. Another major airport implementing a hybrid staffing model explicitly prohibits contract security personnel from touching people or searching bags, limiting contractors to operating x-ray equipment and confirming automated detection displays. This approach removes critical decision-making and searching functions from contractor roles to minimize liability exposure.

However, choosing TSA referral over conducting pat-downs can trigger regulatory documentation requirements. Airports selecting this approach must coordinate with local FSDs and may need to formalize these arrangements in their ASPs, creating a regulatory obligation from what began as a liability mitigation strategy. One airport worked extensively with TSA to document chain-of-custody procedures in their ASP, describing this as their “biggest hurdle.” The documented protocol must specify the complete escalation path from initial alarm through TSA assumption of responsibility. This approach requires agreement from the local FSD. When one airport's request to escort employees to the TSA checkpoint for pat-down resolution was denied, the airport was required to implement its own pat-down procedures.

⁷⁴ A lesser offense of **Criminal Trespass** with a deadly weapon under **Texas Penal Code § 30.05** (Class A misdemeanor) could also potentially apply.

For ASP documentation implications of TSA checkpoint referrals, see Section 12.1.2. For operational implementation of alarm resolution procedures, see Section 9.1.5.

13.1.4 Pat-Down Procedures and Risk Mitigation

Among airports that conduct pat-downs, legal departments have developed specific protocols to minimize liability exposure while maintaining screening effectiveness. One major airport's legal department conducted an in-depth study of pat-down liability and worked with public safety to develop procedures specifying that only trained airport security officers—not contractors—would be authorized to conduct physical searches according to established policy.

Airports have established various limitations on pat-down scope and authority. One airport permits pat-downs only in non-sensitive areas (avoiding chest, groin, and buttocks) and requires verbal consent before any physical contact. Another airport distinguishes between sensitive and non-sensitive areas based on state law requirements, with supervisors typically being the only personnel authorized to conduct limited back-of-hand pat-downs for non-sensitive areas. Multiple airports reported providing pat-down alternatives for employees with medical conditions affecting magnetometer use, directing these individuals to TSA checkpoints for appropriate accommodation.

Gender-specific requirements represent another critical risk mitigation strategy. Multiple airports have implemented policies requiring same-gender pat-downs, with one major airport initially maintaining a 50/50 male/female staffing ratio to ensure adequate coverage before technology solutions reduced physical screening needs. Another airport using contractors has contractual requirements for both male and female staff presence at all times to ensure gender-appropriate screening capability. One airport reported that initial gender-specific screening challenges required policy refinement and additional training to ensure consistent application.

For detailed discussion on operational procedures, see Section 9.1.

13.1.5 Insurance and Risk Transfer Considerations

A number of airports highlighted the importance of engaging with insurance carriers regarding full employee screening implementation. One airport worked closely with their insurance carrier to understand coverage implications and potential premium adjustments related to employee screening activities. Airports reported that proactive engagement with insurance providers helped identify coverage gaps and secure appropriate protection for screening operations.

13.1.6 Camera Coverage and Documentation

Video documentation of screening activities supports quality assurance and liability protection. One airport implemented body cameras to document screening interactions and protect against false claims, reporting no legal challenges since implementation. One major airport reported that screening rooms are fully equipped with cameras, including cameras positioned over search tables, specifically for protecting staff and employees while reducing false allegations. Camera systems provide both real-time oversight capabilities and critical documentation for incident review and legal defense.

13.1.7 Privacy Protections

Employee screening programs must reconcile security requirements with privacy protections. Several research airports incorporated specific privacy protections into their programs. Multiple airports addressed privacy considerations in screening procedures, providing clear guidance on handling

sensitive situations and maintaining professional, respectful environments. Others implemented detailed documentation procedures while ensuring sensitive personal information remained protected.

Transparent communication about privacy policies is key to addressing concerns. One airport reported that thorough communication plans and clear establishment of legal authority helped prevent privacy challenges. Similarly, other airports attributed the absence of privacy challenges to transparent communication approaches that clearly explained screening purposes, procedures, and privacy protections.

For detailed discussion of strategic communications and stakeholder collaboration approaches, see Section 5.1.

13.1.8 Employee Rights and Workplace Accommodations

Employee screening programs must respect employee rights while maintaining security effectiveness. Airports identified several considerations related to employee rights and labor implications during program implementation.

RELIGIOUS ACCOMMODATIONS

A number of airports reported addressing requests for religious accommodation in their screening programs. One major airport handles religious accommodation requests through a TSA checkpoint option, providing alternative screening methods when needed. Airports developed protocols for respectful handling of religious garments and articles during screening processes.

DISABILITY ACCOMMODATIONS

ADA considerations emerged as important program elements. Multiple airports reported considering ADA implications in program design, ensuring screening alternatives were available for those needing accommodations. Airports established procedures for screening employees with medical implants, mobility aids, or other disability-related considerations.

13.2 Recommendations and Implementation Guidance

1. ESTABLISH CLEAR LEGAL AUTHORITY AND FRAMEWORK

Develop a comprehensive legal framework that establishes clear authority for employee screening while ensuring constitutional compliance.

Implementation Guidance: Begin by conducting a thorough legal review with counsel to identify applicable federal, state, and local laws governing employee searches at your airport. Document the administrative search rationale, establishing how employee screening serves special needs beyond normal law enforcement. Ensure your program satisfies the reasonableness test by balancing government interests in aviation security against individual privacy expectations. Develop written policies that clearly articulate the legal basis for screening, scope of searches permitted, and constitutional limitations. Consider whether local ordinances or state statutes provide additional search authority or impose restrictions. Work with legal counsel to ensure screening procedures maintain proportionality between security objectives and privacy intrusions. Consider whether strategic modifications to secured area boundaries could strengthen enforcement authority under state criminal trespass laws, particularly for weapons violations. Document how your program applies screening requirements uniformly to avoid discrimination claims. Establish clear boundaries for what constitutes consent to search as a condition of employment versus voluntary submission to screening.

2. IMPLEMENT COMPREHENSIVE LIABILITY RISK MANAGEMENT

Develop multi-layered strategies to minimize liability exposure while maintaining effective security screening.

Implementation Guidance: Consider implementing a no-touch policy where screening personnel avoid physical contact, instead using technology-based screening methods and referring unresolved alarms to TSA or law enforcement. If pat-downs are necessary, establish detailed protocols specifying authorized personnel, acceptable techniques limited to non-sensitive areas, gender-specific requirements, and documentation procedures. Install comprehensive camera systems covering all screening areas, ensuring both real-time monitoring capability and recorded documentation for incident review. Develop clear chain-of-custody procedures for employees referred to TSA checkpoints, including tracking forms and compliance verification. Create detailed incident response protocols that clearly delineate responsibilities between airport personnel, TSA, and law enforcement. Consider pursuing Safety Act designation if your program meets eligibility requirements, recognizing this requires extensive documentation but provides significant liability protections. Engage early with insurance carriers to understand coverage implications and secure appropriate protection for screening activities. Implement regular audits of screening procedures to identify and address potential liability concerns before they result in claims.

3. DESIGN PRIVACY-CONSCIOUS SCREENING PROGRAMS

Incorporate privacy protections throughout program design and implementation while maintaining security effectiveness.

Implementation Guidance: Conduct a privacy impact assessment during program planning to identify how screening procedures affect employee privacy and develop appropriate mitigation strategies. Establish clear policies limiting the collection, use, and retention of personal information obtained during screening. Implement technical and procedural safeguards to protect sensitive information, including restricted access to screening records and secure storage of documentation. Develop transparent communication materials explaining screening purposes, procedures, privacy protections, and employee rights. Create separate, private screening areas for employees requiring additional screening or accommodation. Train screening personnel on privacy requirements, emphasizing respectful treatment and professional conduct.

4. DEVELOP ROBUST ACCOMMODATION PROCEDURES

Establish processes for addressing religious, disability, and other accommodation needs while maintaining security standards.

Implementation Guidance: Establish clear procedures for employees to request accommodation, including designated points of contact and required documentation. For religious accommodations, develop protocols for respectful handling of religious garments and articles, considering options such as private screening areas or alternative screening methods through TSA checkpoints. For disability accommodations, consider providing alternative screening methods for employees with medical implants, mobility aids, or other disability-related needs. Train screening personnel on accommodation procedures, emphasizing respectful treatment and maintaining dignity during alternative screening. Document all accommodation requests and resolutions.

SECTION 13 QUICK REFERENCE

- Establish clear legal authority grounded in administrative search doctrine
- Implement multi-layered liability risk management strategies including no-touch policies
- Design privacy-conscious programs with formal impact assessments
- Develop robust accommodation procedures for religious and disability needs
- Create comprehensive employee communication and education programs

REFERENCES

- Airport Cooperative Research Program. 2010. Airport Passenger Terminal Planning and Design, Volume 1: Guidebook (Airport Cooperative Research Program (ACRP) Report 25). Washington, DC: National Academies Press.
- Aviation Security Advisory Committee (ASAC). Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control. Washington, DC: Transportation Security Administration, April 8, 2015.
- ASAC. Final Report of the Aviation Security Advisory Committee: Improving Checkpoints at U.S. Airports. May 24, 2017.
- Baeriswyl, Sophie, Andreas Krause, and Adrian Schwaninger. "Emotional Exhaustion and Job Satisfaction in Airport Security Officers – Work–Family Conflict as Mediator in the Job Demands–Resources Model." *Frontiers in Psychology* 7 (May 2016): 663. <https://doi.org/10.3389/fpsyg.2016.00663>.
- Bender, Gloria, Andy Entrekin, Jim Welna, and Jessica Gafford. *Security, Operations, and Design Considerations for Airside Vehicle Access Gates (PARAS 0039)*. Washington, DC: National Safe Skies Alliance, August 2022.
- Bender, Gloria, Andy Entrekin, Jessica Gafford, and Christian Samlaska. *Exit Lane Strategies and Technology Applications*. PARAS 0023. Washington, D.C.: National Safe Skies Alliance, 2021.
- Burrell, Scott A., and Thomas D. Bridenbaugh. "Legal Issues Relating to Airport Commercial Contracts." ACRP Legal Research Digest 41, Transportation Research Board of the National Academies of Sciences, Engineering, and Medicine, Washington, D.C., 2021. <https://doi.org/10.17226/26083>.
- Burns Engineering. *Recommended Security Guidelines for Airport Planning, Design, and Construction*. PARAS 0028, National Safe Skies Alliance, February 2021.
- Chavaillaz, Alain, Adrian Schwaninger, Stefan Michel, and Juergen Sauer. "Work Design for Airport Security Officers: Effects of Rest Break Schedules and Adaptable Automation." *Applied Ergonomics* 79 (2019): 66–75. <https://doi.org/10.1016/j.apergo.2019.04.004>.
- Crosby, Mark, Michael Steinle, Kori Nobel, and Theresa Smith. *Airport Security Vulnerability Assessments*. PARAS 0016. National Safe Skies Alliance, Inc., June 2020.
- Davis, Marc. "The Impact of 9/11 on Business." *Financial Edge*, Investopedia, 2022.
- DeGraw, Donald, Leah Whitfield, Ashlyn Young, Justin Heid, Meg Jones, and Jeffrey Price. *Guidance for Developing and Maintaining an Airport Security Program*. PARAS 0056. Washington, DC: National Safe Skies Alliance, 2024.
- Federal Aviation Administration (FAA). *Airport Improvement Program (AIP) Handbook*. FAA Order 5100.38D, Change 1. Washington, DC: FAA, February 26, 2019.
- FAA. *National Plan of Integrated Airport Systems (NPIAS), 2023–2027*. September 2023. <https://www.faa.gov/sites/faa.gov/files/npias-2023-2027-narrative.pdf>
- FAA. *Passenger Facility Charge (PFC) Program*. Accessed September 29, 2025. <https://www.faa.gov/airports/pfc>.
- FAA. *Updated Reauthorization Program Guidance Letter (R-PGL) 19-02: Planning and Project Eligibility*. Washington, DC: FAA, March 4, 2022.

- Flamenbaum, Harold, Dave Fleet, Ross Gaisor, and Zach Varwig. *Employee Inspections Synthesis Report*. PARAS 0006. National Safe Skies Alliance, Inc., February 2017.
- Friedman, Jordan, Joel Guerrero, Kyle King, Mia Stephens, Michele Freadman, and Richard L. Duncan. *PARAS 0049: Creating and Maintaining a Strong Security Culture at Airports*. PARAS, National Safe Skies Alliance, Inc., September 2023.
- Gill, Charlotte, Julie Hibdon, Cynthia Lum, Devon Johnson, Linda Merola, David Weisburd, Breanne Cave, and Jaspreet Chahal. *TSA's Security Playbook: Phase 2 Technical Report: Results of a National Survey of Playbook and Security Implementation at Category X, I, and II Airports*. George Mason University, January 2012.
- Government Accountability Office (GAO). *A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*. GAO-09-399. Washington, DC: GAO, 2009.
- GAO. *Airport Infrastructure: Information on Funding and Financing for Planned Projects*. GAO-20-298. Washington, DC: Government Accountability Office, February 2020.
- GAO. Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates." Report to Congressional Requesters. GAO-16-632. Washington, D.C.: GAO, 2016.
- GAO. *Aviation Security: TSA Has Policies That Prohibit Unlawful Profiling But Should Improve Its Oversight of Behavior Detection Activities*. GAO-19-490T. Testimony before the Committee on Homeland Security, House of Representatives by William Russell, Acting Director, Homeland Security and Justice. Washington, DC: GAO, 2019.
- GAO. *Aviation Security: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals*. Report to Congressional Requesters. GAO-20-275. Washington, DC: GAO, February 2020.
- GAO. *Airport Worker Screening: TSA Could Further Strengthen Its Approach to Estimating Costs and Feasibility of Security Measures*. Report to Congressional Committees, GAO-21-273. Washington, DC: GAO, 2021.
- GAO. *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*. GAO-20-195G. Washington, DC: GAO, 2020.
- GAO. *Leading Practices: Agile Portfolio Management and Iterative Business Cases Drive Innovative Product Development*. GAO-25-107130. Washington, DC: GAO, 2025.
- Greco, J. Peter. "Insider Threat: The Unseen Dangers Posed by Badged Airport Employees and How to Mitigate Them." *Journal of Air Law and Commerce* 82, no. 4 (2017): 717-742.
- House Homeland Security Committee. "America's Airports: The Threat From Within." Majority Staff Report. Washington, DC: February 2017.
- Houston, Scott, Lee Kair, Gloria Bender, Jessica Gafford, Andy Entrekin, Michele Freadman, and Kim Dickie. *Optimizing Compliance with Airport Security Rules and Regulations*. PARAS 0054. Washington, DC: National Safe Skies Alliance, January 2025.
- Howick, Jodi L. *The Fourth Amendment and Airports*. Transportation Research Board, Airport Cooperative Research Program, Legal Research Digest 27. Washington, DC: National Academies of Sciences, Engineering, and Medicine, 2016.

- Interagency Security Committee. *Best Practices for Planning and Managing Physical Security Resources: An Interagency Security Committee Guide*. Washington, DC: U.S. Department of Homeland Security (DHS), 2015.
- Interagency Security Committee. *Cost Analysis Template*. Excel spreadsheet. Washington, DC: DHS, 2023. https://www.cisa.gov/sites/default/files/2023-02/ISC_Making_a_Business_Case%E2%80%93Cost_Analysis_Template.xlsx.
- Interagency Security Committee. *Making a Business Case for Security: An Interagency Security Committee Best Practice*. 2023 ed. Washington, DC: DHS, 2023.
- International Civil Aviation Organization. *Annex 17 to the Convention on International Civil Aviation: Security—Safeguarding International Civil Aviation Against Acts of Unlawful Interference*. Amendment 17. Adopted 25 November 2019; effective 30 March 2020; applicable 30 July 2020.
- International Civil Aviation Organization (ICAO). “Implementation of 100 Per Cent Screening of Persons Other Than Passengers.” Working Paper presented at the High-Level Conference on Aviation Security (HLCAS), Montreal, September 12-14, 2012.
- ICAO. “Recognition of Equivalence of Security Measures One-Stop Security.” OSS-2023. International Civil Aviation Organization, 2023.
- ICAO. “Settlement of Disputes under Chapter XVIII of the Chicago Convention.” ICAO: Frequently Asked Questions. Accessed February 28, 2025. <https://www.icao.int/about-icao/FAQ/Pages/settlement-of-disputes-under-chapter-xviii-of-the-chicago-convention.aspx>.
- InterVISTAS Consulting USA LLC and Baldwin Liaison Consulting. *Planning and Design Considerations for International Arrivals Facilities: Implementing CBP's Airport Technical Design Standard*. PARAS 0052, August 2024. National Safe Skies Alliance, Inc.
- Kruger, Jenny Kathinka, and Boris Suchan. “Humans Are Still the Critical Factor in Aviation Security.” *Aerospace Medical Association*, 2015. <https://www.researchgate.net/publication/283204186>
- Maruf, Harun. “Somali Plane Bomb: What Happened?” BBC News, February 13, 2016. <https://www.bbc.com/news/world-africa-35521646>.
- McGee, Sibel, Ph.D. (PI), Peggy McCarthy, and Analytic Services Inc. (ANSER). *Guidance for Root Cause Analysis in Aviation Security (PARAS 0027)*. Falls Church, VA: National Safe Skies Alliance, January 2021.
- Morral, Andrew R., Brian A. Jackson, Peter J. E. Stan, John S. Hollywood, Henry H. Willis, Tom LaTourrette, and Mel Eisman. *Modeling Terrorism Risk to the Air Transportation System: An Independent Assessment of TSA's Risk Management Analysis Tool and Associated Methods*. Santa Monica, CA: RAND Corporation, 2012. <https://www.rand.org/pubs/monographs/MG1241.html>.
- National Academies of Sciences, Engineering, and Medicine. 2007. Synthesis 1: *Innovative Finance and Alternative Sources of Revenue for Airports*. Washington, DC: The National Academies Press.
- National Safe Skies Alliance, Inc. PARAS 0011: *Guidance for Airport Security Master Planning*. Program for Applied Research in Airport Security, January 2019.
- National Safe Skies Alliance. *PARAS 0016: Airport Security Vulnerability Assessments (SVA) Guidebook*. Washington, DC: Program for Applied Research in Airport Security, 2018.

- Nelson, Nicole. 2015. "Atlanta Int'l Takes Aim at Insider Threats with Full Employee Screening." *Airport Improvement*, November/December 2015.
- "OIA Part of Probe into Drug Smuggling," *Orlando Sentinel*, September 17, 2009, updated August 6, 2021, <https://www.orlandosentinel.com/2009/09/17/oia-part-of-probe-into-drug-smuggling/>.
- Ritchey, Diane. "Employee Screening Boosts Security at Miami Airport." *Security Magazine*, July 1, 2015.
- Salus Solutions. (2021). *Insider Threat Mitigation at Airports* (PARAS 0026). National Safe Skies Alliance.
- Swann, Levi, Vesna Popovic, Alethea Blackler, and Helen Thompson. "Airport Security Screener Problem-Solving Knowledge and Implications." *Human Factors* 61, no. 8 (2019): 1262–1284. <https://doi.org/10.1177/0018720819874169>.
- Texas Penal Code Annotated*. St. Paul, MN: Thomson Reuters, 2023.
- Thompson, Bennie G. "A Review of Access Control Measures at Our Nation's Airports, Part II." Statement before the Transportation Security Subcommittee of the U.S. House Committee on Homeland Security, April 30, 2015.
- Transportation Security Administration (TSA). *Insider Threat Roadmap 2020*. Washington, DC: DHS, 2020. Accessed October 2, 2025. https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf
- TSA. "One Stop Security' Pilot Program Aims to Simplify International Travel." August 27, 2025. Accessed October 2, 2025. <https://www.tsa.gov/news/press/releases/2025/08/27/one-stop-security-pilot-program-aims-simplify-international-travel>.
- TSA. "SIDA Airport Security: Fiscal Year 2017 Report to Congress." Washington, DC: DHS, February 6, 2018.
- TSA. "What Can I Bring?" Accessed January 16, 2026. <https://www.tsa.gov/travel/security-screening/whatcanibring/all>.
- Trethewey, Neil, Michele Freadman, Kim Dickie, Craig Lynes, and Rose Marengo. *Strategies for Developing an Aviation Worker Screening Program*. PARAS 0060. Washington, DC: National Safe Skies Alliance, Inc., July 2024.
- United States Code. *Title 49—Transportation, Subtitle VII—Aviation Programs, Part A—Air Commerce and Safety, Subpart ii—Economic Regulation, Chapter 401—General Provisions, § 40117. Passenger Facility Charges*.
- U.S. House of Representatives. Committee on Homeland Security, Subcommittee on Transportation Security. "Lessons from the LAX Shooting: Preparing for and Responding to Emergencies at Airports." 113th Congress, Washington, DC, March 28, 2014. <https://www.govinfo.gov/content/pkg/CHRG-113hhrg88559/html/CHRG-113hhrg88559.htm>.
- U.S. Department of Homeland Security, Office of Inspector General. "TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening." OIG-09-05, October 2008.
- U.S. Department of Justice. "Twelve Current and Former TSA and Airport Employees Indicted for Smuggling Approximately 20 Tons of Cocaine." Press Release. U.S. Attorney's Office, District of Puerto Rico, February 13, 2017. <https://www.justice.gov/usao-pr/pr/twelve-current-and-former-tsa-and-airport-employees-indicted-smuggling-approximately-20>.

U.S. General Services Administration. “GSA Cooperative Purchasing Program.” Accessed October 15, 2025.
<https://www.gsa.gov/buy-through-us/purchasing-programs/programs-for-state-and-local-government/cooperative-purchasing-program>.

U.S. General Services Administration. “Learn about the 1122 Program.” Accessed October 15, 2025.
<https://www.gsa.gov/buy-through-us/purchasing-programs/programs-for-state-and-local-government/1122-program>

United States. H.R.876 - Aviation Employee Screening and Security Enhancement Act of 2017. 115th Congress (2017-2018).

United States. FAA Reauthorization Act of 2018. Public Law 115-254. 132 Stat. 3186. October 5, 2018.

Zoufal, Don, Sean Cusson, Michele Freadman, Douglas Wendt, Jessica Gafford, and Mary Ann Pantle. *Strategies for Aviation Security Stakeholder Information Sharing*. PARAS 0044, June 2023. National Safe Skies Alliance, Inc.

Zoufal, Don, Kevin Whitney, Erin Manning, Mary Ann Pantle, Robert Boblitz, Richard Duncan, and Sean Cusson. *Implementing Biometric Technology at Airports*. PARAS 0045, February 2024. Chicago, IL: National Safe Skies Alliance, Inc.

APPENDIX A: SAMPLE QUALITY ASSURANCE FORMS FOR EMPLOYEE SCREENING OPERATIONS

The following Quality Assurance (QA) forms were developed by a participating airport to evaluate screener competency through structured assessments. These forms demonstrate a systematic approach to performance evaluation that assesses screening personnel across three dimensions:

- **Knowledge:** Understanding of policies, SOPs, device capabilities, and procedural requirements for each screening function
- **Communication:** Ability to provide clear verbal instructions to aviation workers and explain procedures appropriately
- **Skills/Alarm Resolution:** Practical demonstration of proper screening techniques and ability to resolve common alarm scenarios

The five forms address core screening functions that airports may incorporate into their full employee screening programs:

1. Two-Factor Authentication
2. Personnel Screening
3. Personal Property Screening
4. ETD
5. TSA Checkpoint Escort Procedures

Each form includes specific competency items that can be assessed using checkboxes for Yes, No, and N/A, enabling consistent evaluation across all screening personnel. The forms also include signature blocks for both the officer being evaluated and the certifying evaluator, supporting documentation requirements for annual recertification programs.

Airports developing or enhancing their QA programs can adapt these forms to align with their specific equipment configurations, procedures, organizational terminology, and prohibited item policies. Bracketed terms indicate airport-specific references that should be replaced with local terminology.

1. Aviation Worker Personnel Screening: Two-Factor Authentication

The purpose of screening Aviation Workers is to prevent prohibited items and unauthorized persons from entering the sterile and secure areas via Access Points.

Did the officer performing the screening accomplish the following? YES NO N/A

Two-Factor Authentication

1. Knowledge:

- Ability to explain how the two-factor authentication device works and knowledgeable on procedures:
 - i. Uses two-factor authentication (SIDA badge and facial recognition)
 - ii. Facial recognition enrollment via *[airport access control office]* and is unique to each badge-holder.
 - iii. Cameras on device scans face geometry.
 - iv. Capable of coping to changes (change of hairstyle, glasses, facial hair)
 - v. Possible obstructions and considerations (safety goggles, position of head wear, delay time from scanning to positioning face, etc.)
 - vi. Procedure for "Access Denied"

☐ ☐ ☐

2. Communication:

- Security personnel will instruct aviation worker to approach the two-factor facial recognition device:
 - i. Stand in front of device (approximately arms-length)
 - ii. Scan SIDA badge at the bottom of device
 - iii. Stand straight and look in the direction of the cameras located at the top of the device.
 - iv. Wait for "Access Granted" message and green status bar.
 - v. Instruct aviation worker to visit *[airport access control office]* for "Access Denied."

☐ ☐ ☐

3. Skills – Alarm Resolution:

- Demonstrate ability to provide verbal instructions on using device.
- Demonstrate ability to resolve potential issues (access denied, scanning timeout, mismatch – another badge-holder standing too close in camera view)

☐ ☐ ☐

PASS FAIL

Officer Signature: _____

Certified by: Name: _____ Signature: _____

2. Aviation Worker Personnel Screening

The purpose of screening Aviation Workers is to prevent prohibited items and unauthorized persons from entering the sterile and secure areas via Access Points.

Did the officer performing the screening accomplish the following?

YES NO N/A

Personnel Screening Device

1. Knowledge:

☐ ☐ ☐

- Policy competency: reviewed Limited Pat Downs Policy/SOP.
- Ability to explain how the personnel screening device works:
 - i. Device capabilities (walk-through, scans for body anomalies using millimeter wave technology, not harmful and safe on medical devices, on-person alarm(s) are identified via operator's display monitor)
 - ii. Resolving on-person alarm(s)
 - iii. Rescreening process for on-person alarm(s)
 - iv. Minimal disruptions in queue
 - v. Limited pat down for alarm(s) that cannot be resolved by divesting or reinitiating screening.
 - vi. Opposite gender alarm resolution.
 - vii. Identify non-sensitive vs. sensitive area(s) of a person's body.
 - viii. Critical on-person alarm(s) for compliant vs. non-compliant individual.
 - ix. TSA resolution for on-person alarm(s) that cannot be resolved.

2. Communication:

☐ ☐ ☐

- Security personnel will provide announcements advising aviation workers to walk through the personnel screening device with arms at their side, walking at a moderate pace.
- In the event of on-person alarm(s), security personnel will provide verbal instructions to aviation worker to remove item(s) causing alarm.
- Educate aviation worker on cause of alarm(s) and prevention tips to create a positive experience moving forward.

3. Skills – Alarm Resolution: (Demonstrate limited pat down)

☐ ☐ ☐

- On-person alarm(s) may be resolved by additional divesting or rescreening:
 - i. Allow aviation worker to remove alarmed item(s) and submit to rescreening.
 - ii. If the alarm(s) cannot be resolved by divesting or rescreening, a limited pat down will be offered.

	YES	NO	N/A
○ Upon consent, limited pat downs will only be conducted by security personnel of the same gender and only on non-sensitive area(s) as indicated by an on-person alarm. Security personnel will position the aviation worker in the designated area to perform the limited pat down. <u>Exception: Opposite gender alarm resolution will be cleared with self-pat down and Explosive Trace Detection (ETD)</u> ○ Alarms identified on sensitive areas of the body will be referred to TSA for resolution. Limited pat downs <u>will not be</u> conducted on sensitive areas of the body.	☐	☐	☐
4. Notify Supervisor and complete Incident Report.	☐	☐	☐

PASS FAIL

Officer Signature: _____

Certified by: Name: _____ Signature: _____

3. Aviation Worker Personal Property Screening: X-ray & Automated Threat Detection

The purpose of screening Aviation Workers is to prevent prohibited items (PI) and unauthorized persons from entering the sterile and secure areas via Access Points.

Did the officer performing the screening accomplish the following?

YES NO N/A

X-ray & Automated Threat Detection

1. Knowledge:

☐ ☒ ☐

- Policy competency: reviewed Personal Property Screening & Alarm Resolution Policy/SOP.
- Ability to explain how X-ray and Autonomous AI detection works:
 - i. All monitor(s) will be turned off except for the monitor(s) operating Autonomous AI.
 - ii. Explain vendor recommended calibration of the X-ray machine.
 - iii. *[Authorized Security Personnel]* will notify the on-site *[security resolution personnel]* to assist in locating suspected prohibited items (PI) identified by *[advanced threat detection]*, which must be resolved by a physical bag inspection or police response.
 - iv. Explain the different functions (Mark, Send to Review, No PI, Report PI)
 - v. Explain the process if *[automated threat detection]* detects non-dangerous vs. dangerous item(s).
- Purpose of having 2 X-ray lanes and when to pause/resume operations.
 - i. Resolution Officer will resolve alarms to maintain continuous flow.
 - ii. Screening will only pause for non-compliant/critical items
- Demonstrate startup, login, testing conveyor belt, test kit, calibration, and shutdown.
- Identify conveyor belt controls and emergency stops, including and how to reset.

2. Communication:

☐ ☐ ☐

- Security personnel will provide announcements advising aviation workers that all personal items will be screened through x-ray machine.
 - i. Loose items must be placed in their bag/backpack/purse or bin.
 - ii. No items will be allowed in the hands during the personnel screening process.
 - iii. Workers may avoid removing access badges on clean lanyards around the neck and/or wristwatches.
 - iv. Large, bulky items which may conceal firearms, tactical knives, and explosives must be taken off and submitted through property screening.
 - v. Prior to physical bag inspection on alarmed item(s), security personnel must ask the aviation worker if there are any weapons, explosives, incendiaries, or PI, including any sharp or harmful items.

YES NO N/A

3. Skills – Alarm Resolution:☐ ☐ ☐

- Alarm (**audible buzzer sound with display on “Inspect” monitor**)
 - i. All suspected weapons, explosives, incendiaries, or PI identified by Autonomous AI must be resolved.
 - ii. If the X-ray operator is unable to positively identify any threat alarm, they shall follow standard bag search procedures. X-ray operator will pause X-ray operations and contact *[resolution personnel]* to perform physical bag inspection to identify alarmed item(s).
 - iii. Clearly identifiable item(s) that are non-dangerous (i.e., water bottles) will not be hand searched and will be cleared on the “Inspect” monitor as “No PI.”
 - iv. Non-dangerous PI: send to “Review” monitor and conduct bag inspection.
 - v. Dangerous PI: stop conveyor belt immediately, keep PI in X-ray tunnel, and notify *[Security Coordination Center]* for Police response.

4. Portal Violation & Reporting Matrix:☐ ☐ ☐

- Non-critical/No TSA Notification
(Escort aviation worker out of access point, Return PI, No Police Response, Notify Supervisor, Incident Report)
- Non-critical with TSA Notification
(Escort aviation worker out of access point, Return PI, No Police Response, Notify Supervisor, Incident Report)
- Critical with TSA Notification
(Maintain positive control of item(s), Police Response Required, Notify Supervisor, Incident Report)

Operations will resume at Police or [Airport Security Authority's] discretion.

PASS FAIL

Officer Signature: _____

Certified by: Name: _____ Signature: _____

4. Aviation Worker Screening: Explosive Trace Detection (ETD)

The purpose of screening Aviation Workers is to prevent prohibited items and unauthorized persons from entering the sterile and secure areas via Access Points.

Did the officer performing the screening accomplish the following? YES NO N/A

ETD

1. Knowledge:

☐ ☐ ☐

- Policy competency: reviewed ETD Policy/SOP.
- Ability to explain the ETD procedure:
 - i. Device capabilities (detects explosive traces)
 - ii. Understands device startup, warmup, calibration, verification process is completed by *[airport security supervisors]* or a designated security personnel.
 - iii. Understands general care and maintenance of device.
 - iv. Using gloves and when to discard.
 - v. Correct orientation when handling traps.
 - vi. Reuse vs. disposal of traps.
 - vii. Collecting samples via traps:
 - Hand sampling
 - Bottle sampling
 - Opposite gender self-pat down sampling
 - Religious headgear that cannot be removed
 - viii. Positive sample vs Negative sample procedure
 - ix. Refusal
 - x. Notification for Police response
 - xi. Pause and resume operations

2. Communication:

☐ ☐ ☐

- Inform aviation worker that he/she was selected for additional screening.
- Provide verbal instructions:
 - i. Both hands out with palms facing up; fingers together (including thumbs)
 - ii. Place bottle on table (if applicable)
 - iii. Opposite gender: self-pat down of non-sensitive areas prior to sampling
 - iv. Religious headgear: self-pat down of religious headgear prior to sampling

	YES	NO	N/A
--	-----	----	-----

3. Skills – Sampling:

- Demonstrate sample collection using traps.
- Insert trap into ETD in the correct orientation.
- 4 swipes per hand; 8 total
- 6 swipes per bottle

☐	☐	☐
--------------------------	--------------------------	--------------------------

PASS	FAIL
------	------

Officer Signature: _____

Certified by: Name: _____ Signature: _____

5. Aviation Worker Screening: Escorting to TSA Checkpoint

The purpose of screening Aviation Workers is to prevent prohibited items and unauthorized persons from entering the sterile and secure areas via Access Points.

Did the officer performing the screening accomplish the following?

YES NO N/A

Escorting to TSA Checkpoint

1. Knowledge:

☐ ☐ ☐

- Policy competency: reviewed Escorting to TSA Checkpoint Policy/SOP.
- Ability to explain the process:
 - i. On-person alarm(s) that cannot be resolved at Aviation Security Access Point must be resolved by escorting aviation worker to TSA checkpoint for resolution.
 - By request of the aviation worker, or
 - An alarm indicated in a sensitive area that cannot be resolve
- Procedure for TSA hand-off:
 - i. Escort aviation worker to front of line and request TSA Supervisor.
 - ii. Clearly describe area(s) that were unable to be cleared.
 - iii. Request liquid exemption, if applicable.
 - iv. Provide TSA with security screening card.
 - v. Ensure escort log is completed.
- Procedure for aviation worker who refuses to be escorted to TSA Checkpoint.
 - i. Do not follow
 - ii. Immediate notification to *[Security Coordination Center]* requesting Police response and suspension of badge.
 - iii. Describe situation, description of individual and direction of travel.

2. Communication:

☐ ☐ ☐

- Security personnel will communicate escorting process for unresolved alarms:
 - i. Collect all personal property.
 - ii. Inform aviation worker that TSA screening standards are different and will be performed to TSA's discretion.
 - iii. Inform aviation worker of Security Screening Card – unique identification card issued to individuals proving the holder has undergone the requisite security checks at a TSA Checkpoint.

3. Skills:

☐ ☐ ☐

- Demonstrates ability to identify alarm(s) in sensitive area(s) that require resolution at TSA Checkpoint.
- Notify Supervisor and complete Incident Report.

PASS

FAIL

Officer Signature: _____

Certified by: Name: _____ Signature: _____