PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0056 October 2024

Guidance for Developing and Maintaining an Airport Security Program

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Donald DeGraw
Leah Whitfield
Ashlyn Young
Justin Heid
The Aviation Planning Group, LLC
Fredericksburg, Virginia

Meg Jones
Ardurra
Boise, Idaho

Jeffrey C. Price
Leading Edge Strategies
Arvada, Colorado

NOTICE

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

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

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

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

NATIONAL SAFE SKIES ALLIANCE, INC.

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

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

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

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

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

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

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

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

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

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

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

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0056 PROJECT PANEL

Martina Benedikovicova *Charlotte Douglas International Airport*
Andy Entrekin *TransSolutions, LLC*
Lance Ferrell *M2P Consulting*
Joseph Gaudio *SSi, Inc*
Scott Lawrence *Metropolitan Airports Commission*
Bill Marrison *McGhee Tyson Airport (Retired)*
Rob McQueen *Rob McQueen Consulting*
Enrique Melendez *The JW Group*
Jodi Spencer *Boise Airport*
Nikola Vucicevic *John F. Kennedy International Airport*
Andrew Young *Chrysalis Global Aviation*

AUTHOR ACKNOWLEDGEMENTS

The research conducted for this project was performed by The Aviation Planning Group, LLC; Ardurra; and Leading-Edge Strategies, LLC.

The Aviation Planning Group team was led by Donald DeGraw, who was the Principal Investigator for the project. Leah Whitfield was the Administrative Officer and conducted airport outreach interviews, developed content, performed quality control reviews, and provided administrative functions. Justin Heid provided content input and performed quality control reviews. Ashlyn Young aided with organizing, editing, and formatting the report.

The Aviation Planning Group would like to thank their teammates in this project, Ardurra and Leading-Edge Strategies. Meg Jones from Ardurra conducted airport outreach interviews, developed content, and performed quality control reviews. Jeff Price from Leading-Edge Strategies conducted the literature review, performed airport outreach, developed content, and performed quality control reviews.

The entire team would like to express their appreciation to the airport and TSA security professionals who provided their time and expertise assisting in this project. Their contributions reflect their commitment to the entire aviation community.

The team would also like to recognize the Safe Skies PARAS Program Manager, Jessica Grizzle, the Project Panel, and Safe Skies for their significant contributions of time, effort, and guidance during this project.

CONTENTS

TABLES & FIGURES

SUMMARY

This guidebook provides practical guidance to assist airport operators in developing and maintaining an Airport Security Program (ASP), overcoming challenges related to implementing amendments to an existing ASP, or developing a new ASP due to expanding commercial air service. The project guidance recognizes various approaches for creating or amending an ASP and is structured to efficiently assist airports in developing the appropriate content for an effective Complete, Supporting, or Partial security program. Additionally, the guidance discusses a proactive approach to maintaining an ASP, identifying risks, streamlining processes, and effectively communicating with stakeholders to maximize program effectiveness.[1]

This guidance discusses the following:

- How to develop the program content
- Effective implementation of administrative changes
- Effective program maintenance strategies that will streamline the ASP format and minimize the need for amendments
- The importance of maintaining positive stakeholder relations and suggested strategies for effective ASP-related communications

[1] TSA-NA-01-01 Airport Categorization

PARAS ACRONYMS

ACRP	Airport Cooperative Research 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
IED	Improvised Explosive Device
IT	Information Technology
SIDA	Security Identification Display Area
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ASC	Airport Security Coordinator
ASP	Airport Security Program
ATSP	Airport Tenant Security Program
CHRC	Criminal History Records Check
EAA	Exclusive Area Agreement
FAR	Federal Aviation Regulation
HSIN	Homeland Security Information Network
ICAO	International Civil Aviation Organization
IC	Information Circular
LEO	Law Enforcement Officer
NA	National Amendment
PACS	Physical Access Control System
PIDS	Perimeter Intrusion Detection Systems
PIN	Personal Identification Number
SD	Security Directive
STA	Security Threat Assessment
TOC	Table of Contents

SECTION 1: INTRODUCTION

The Airport Security Program (ASP) is the local foundation for maintaining a secure and cohesive security platform across the nation's airports. Commercial service airports operating under the requirements of an ASP share many similarities but also have unique challenges.

The ASP must contain the proper content to provide the Airport Security Coordinator (ASC) with the tools and resources needed to perform their duties efficiently. The ability to effectively carry out the requirements of an ASP rest heavily on how well the program is written and formatted, as well as having trained staff in place to discharge the requirements of the program. The ASP must clearly identify the requirements for each security area (Secured/AOA/SIDA), the access control system, airport badging, and law enforcement, and respond to TSA Security Directives (SD) and Information Circulars (IC).

Additionally, having an established procedure in place to support temporary operational changes related to construction, VIP events, security incidents, and equipment malfunctions is critical to the functioning of an effective security program.

1.1 Research Methods & Approach

Interviews were conducted with 22 ASCs at airports ranging in size and complexity from Category X to Category IV, as well as four TSA officials from three different TSA Surface Regions. The questions asked during the interviews were designed to comprehensively cover how each airport develops content, implements changes, maintains their program, works with stakeholders, and determines need-to-know criteria. The questions also ascertained their general approach to creating or revising their ASP. Most airports reported having similar challenges in the development and maintenance of their ASP, but the practices each airport used to resolve those challenges tended to vary by airport size and region.

The ASCs were asked ten standard questions and then supplemental questions were asked as the interviews progressed. This provided insight into the strengths and weaknesses of each airport's program. Similarly, the TSA officials who were interviewed provided a balanced view of the approval process and expectations for an effective ASP from the TSA regulatory perspective.

A comprehensive literature review involved identifying existing resources, reviewing relevant literature, reviewing regulatory changes, and documenting publicly available resources. There was not a significant amount of information written about drafting an ASP, and much of the industry's existing guidance is considered SSI. Some public guidance was discovered in textbooks, security certification programs, and PARAS research reports. The literature review included:

- **Research Reports:** Previous ACRP and PARAS projects related to ASPs, plus industry peer-reviewed research through the Journal of Airport Management, and related scholarly works in the field of security management.
- **Security textbooks:** Material on airport security and the development and implementation of ASPs from an International Civil Aviation Organization (ICAO) perspective, plus other security programs such as transportation (rail, maritime), industrial facilities, and other related areas.
- **TSA and ICAO requirements:** A comprehensive review of the requirements related to the development and approval of ASPs.

Due to the limited public information available for ASPs, the review was expanded to also include other similar security and emergency plans, such as FAA Advisory Circulars, FEMA homeland security guidance and in some cases, international guidance.

The cumulation of data from the interviews and literature review, and the lessons learned from the research synthesis were used to develop the deliverables for this project.

For a list of the questions posed to airports and TSA during the interviews, see Appendix C. Literature review findings are in Appendix D.

1.2 How to Use This Report

This report is intended to be used as guidance in developing an ASP, but it does not explain every aspect of an ASP, nor every possible option in ensuring compliance with the regulations. Many airport security processes are published in SSI-protected SDs and TSA local and National Amendments (NA). Airport operators should consult these documents and work closely with TSA to ensure compliance with the regulations, directives, etc. Currently applicable SDs and NAs, as well as additional publications on airport security that airport operators may find helpful in determining methods of compliance are listed in Appendix A.

IMPORTANT: This document only addresses publicly available information. Several of the regulatory requirements have since been changed through TSA-issued SDs and NAs. These documents are designated as SSI and are not available to the general public. Any reader who intends on using this document to implement or modify their ASP is strongly encouraged to review all applicable SDs and NAs, plus any local amendments, prior to making any changes to their ASP.

This report applies to commercial service airports operating under Title 14 CFR § 139 Certification of Airports and Title 49 CFR §1542 Airport Security. The report may also apply to certain airports exempt from Part 139 regulations.

1.3 Key Sections

The sections in this guidance include:

- **Section 2 – Security Program Overview:** This section outlines the security program requirements for each airport security category. It also discusses the roles and responsibilities for the Primary and Alternate ASCs in developing and implementing the ASP.
- **Section 3 – Developing ASP Content:** This section provides the guidance needed to create or amend content for an ASP. It focuses on the formats provided by the TSA in 49 CFR § 1542 Airport Security and other applicable guidance. The guidance can be used to develop a new program, update an existing program, or transition between programs. Recommendations are provided that will assist with content type and the level of detail to be included.
- **Section 4 – Implementing Administrative Changes:** This section provides guidance for amending or establishing a new program with recommended policies and procedures that will facilitate efficient amendment submissions and TSA reviews. This section looks at the root causes for ASP amendments, the associated impacts, and typical triggering events that require a change be made to a program. Recommendations are provided to help streamline TSA approval processes and ensure SSI material is protected.

- **Section 5 – Program Maintenance Strategies:** This section provides recommendations focused on policies and procedures that will ensure an airport's ASP is maintained in a current and complete manner. This section looks at routine reviews of security content, updates to SDs & ICs, TSA local & National Amendments, key personnel changes, required testing, recurrent training, and annual exercise reviews. Guidance will also include operational/administrative checklists and recommended timelines for routine administrative reviews.
- **Section 6 – Stakeholder Communication Strategies:** This section will focus on maintaining stakeholder relationships with both internal and external security stakeholders directly responsible for the implementation of the ASP and its directives. It will differentiate between the dissemination of non-SSI information and SSI information to the various stakeholder groups and how developing strong relationships assists in the overall effectiveness of an ASPs mission. Guidance will give recommendations on how to effectively maintain communications with airport stakeholders and TSA partners with security bulletins, meetings, and other outreach tools.

The five appendices in this guidance include:

- **Appendix A - Reference and Guidance Documents for ASCs:** This appendix reference key documents that ASCs should be familiar with during the process of creating or updating an ASP.
- **Appendix B - Glossary:** This appendix provides definitions for key terms used in this document as defined with industry standards and regulatory definitions.
- **Appendix C – Airport & TSA Interview Questions:** This appendix details the questions posed to airport and TSA stakeholders during the interviews.
- **Appendix D - Literature Review Findings:** This appendix details the research and results from the literature review and the sources used.
- **Appendix E - Checklists for Creating and Reviewing the ASP:** This appendix summarizes the 26 items that are required during the creation of an ASP, generally defining specific sections in the ASP document. It also provides a checklist for reviewing the ASP when routine and significant change reviews are performed to ensure the ASP is consistently being maintained in a complete and accurate manner.

SECTION 2: SECURITY PROGRAM OVERVIEW

Each commercial service airport operator is required to implement an ASP, which must be approved by TSA prior to the start of commercial operations.[2] This section focuses on the requirements for the ASP, and the various roles of those tasked with developing and administering the ASP.

The ASP describes how a particular commercial service airport will comply with the regulations under Part 1542. ASPs are unique to each airport, are drafted by the ASC, and prior to implementation must be approved by the TSA's Federal Security Director (FSD). TSA legal counsel may also be involved in ASP approvals or changes. Any unexpected changes or proposed changes to the ASP must be approved by the FSD.

Part 1542 describes *what* the airport operator must comply with, while the ASP describes *how* the individual airport complies with this Part. The ASP must also address compliance with SDs and NAs where applicable. With TSA approval, the SDs and NAs may be included in the ASP's appendices. The ASP is considered SSI; airport operators must limit the sharing, release, and accessibility of SSI, as defined in Part 1520, exclusively to individuals with a need-to-know. Any requests for SSI from other individuals should be directed to TSA.

2.1 Program Requirements

Part 1542.101 General Requirements

(a) no person may operate an airport subject to Part 1542.103 unless is adopts and carries out a security program that—

(1) Provides for the safety and security of persons and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary onto an aircraft;

(2) Is in writing and is signed by the airport operator;

(3) Includes the applicable items listed in § 1542.103;

(4) Includes an index organized in the same subject area sequence as § 1542.103; and

(5) Has been approved by TSA.

(b) Each airport operator subject to § 1542.103 must maintain one current and complete copy of its security program and provide a copy to TSA upon request.

(c) Each airport operator subject to § 1542.103 must—

(1) Restrict the distribution, disclosure, and availability of sensitive security information (SSI), as defined in part 1520 of this chapter, to persons with a need to know; and

(2) Refer all requests for SSI by other persons to TSA.

There are three types of security programs: Complete, Supporting, and Partial. The contents of an ASP vary depending on which of the three security programs is required by TSA for the particular airport. The security program for a commercial service airport primarily depends on the number of passenger enplanements and the nature of the airport's flight operations.[3]

[2] A commercial service airport operates under Federal Aviation Regulation Part 139 (Airport Certification) and hosts a certain level of scheduled service (aircraft operating with 10 or more seats), and/or large unscheduled service flight operations in aircraft operating with more than 30 seats.

[3] TSA-NA-01-01 Airport Categorization

Under CFR § 1542.103(a), **Category X, I, II, and III airports** serving aircraft operations in scheduled passenger or public charter operations with an aircraft having more than 60 seats, or fewer seats when enplaning or deplaning into a Sterile Area, and where TSA provides screening services, are required to have a Complete ASP. Airports serving foreign air carrier operations and possessing a permit from the Department of Transportation are also required to follow the requirements of a **Complete ASP**.

Under CFR § 1542.103(b), any airport with aircraft operations in an aircraft with a **passenger seating configuration of 60 or fewer seats when enplaning into or deplaning from a Sterile Area**, and where TSA provides screening services for those flight operations, are required to follow a **Supporting Airport Operator Security Program**. Any airport where private charter operations are conducted, and where the aircraft operator is enplaning or deplaning passengers from a Sterile Area or has a maximum certificated takeoff weight of more than 100,309.3 pounds, conducting private charters in aircraft with a passenger-seating configuration of 61 or more under the Private Charter Security Program, are also required to follow a **Supporting Security Program**. Any required screening (i.e., passengers and carry-on baggage in the case of a Private Charter Standard Security Program) that is not conducted by TSA must be conducted by an approved entity, such as the aircraft operator.

Under CFR § 1544.101(b)[4] or CFR 1546.101(d),[5] **Category IV airports** with aircraft operations in **scheduled** or **public charter** operations with an aircraft **seating configuration of 31–60 seats**, operating to, from, or outside the United States, but that **do not enplane or deplane into a Sterile Area**, are required to follow the requirements of a Partial ASP. Airports serving foreign aircraft operations of 31–60 seats when TSA has not notified the foreign air carrier in writing that a threat exists to their operation, must also adhere to a **Partial Security Program**. Partial Security Programs are typically used for airports with seasonal, low levels of commercial aircraft operations, such as public charters. During regulated operations, the airport must still provide for uniformed and qualified law enforcement personnel to be present or to respond within the required response times.

The majority of commercial service airports in the US have a Complete program. The majority of Supporting and Partial programs are at commercial service airports that serve predominantly general aviation operations, with just a few commercial operations per day.

Note: the following table is cross-referenced so the numbering sequence may be different from one row to the next. Also, this list identifies the regulatory citations. A simplified version of this list can be found in Table 5-2 in Section 5.1.1.

Table 2-1. Three Types of Security Programs and Requirements

Complete	Supporting	Partial
Except as otherwise approved by TSA, each airport operator regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(1) or § 1546.101(a) of	Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(a)(2) or (f), or § 1546.101(b) or (c) of this chapter,	Except as otherwise approved by TSA, each airport regularly serving operations of an aircraft operator or foreign air carrier described in § 1544.101(b) or § 1546.101(d) of this chapter, must include in its

[4] A scheduled passenger or public charter passenger operation with an aircraft having a passenger-seating configuration of 31 or more but 60 or fewer seats that does not enplane from or deplane into a Sterile Area, or a scheduled passenger or public charter passenger operation with an aircraft having a passenger-seating configuration of 60 or fewer seats engaged in operations to, from, or outside the United States that does not enplane from or deplane into a Sterile Area.
[5] Each flight operation with an airplane having a passenger seating configuration of 31 or more seats but 60 or fewer seats, when TSA has not notified the foreign air carrier in writing that a threat exists with respect to that operation.

Complete	Supporting	Partial
this chapter, must include in its security program the following:	must include in its security program a description of the following:	security program a description of the following:
(1) The name, means of contact, duties, and training requirements of the ASC required under § 1542.3.	(1) Name, means of contact, duties, and training requirements of the ASC, as required under § 1542.3.	(1) Name, means of contact, duties, and training requirements of the ASC as required under § 1542.3.
(2) [Reserved]	(2) [Reserved]	(2) [Reserved]
(3) A description of the secured areas, including— (i) A description and map detailing boundaries and pertinent features; (ii) Each activity or entity on, or adjacent to, a secured area that affects security; (iii) Measures used to perform the access control functions required under § 1542.201(b)(1); (iv) Procedures to control movement within the secured area, including identification media required under § 1542.201(b)(3); and (v) A description of the notification signs required under § 1542.201(b)(6).	X	X
(4) A description of the AOA, including— (i) A description and map detailing boundaries, and pertinent features; (ii) Each activity or entity on, or adjacent to, an AOA that affects security; (iii) Measures used to perform the access control functions required under § 1542.203(b)(1); (iv) Measures to control movement within the AOA, including identification media as appropriate; and (v) A description of the notification signs required under § 1542.203(b)(4).	X	X
(5) A description of the SIDAs, including— (i) A description and map detailing boundaries and pertinent features; and	X	X

Complete	Supporting	Partial
(ii) Each activity or entity on, or adjacent to, a SIDA.		
(6) A description of the sterile areas, including— (i) A diagram with dimensions detailing boundaries and pertinent features; (ii) Access controls to be used when the passenger-screening checkpoint is non-operational and the entity responsible for that access control; and (iii) Measures used to control access as specified in § 1542.207.	X	X
(7) Procedures used to comply with § 1542.209 regarding fingerprint-based criminal history records checks.	X	X
(8) A description of the personnel identification systems as described in § 1542.211.	X	X
(9) Escort procedures in accordance with § 1542.211(e).	X	X
(10) Challenge procedures in accordance with § 1542.211(d).	X	X
(11) Training programs required under §§1542.213 and 1542.217(c)(2), if applicable.	(3) Training program for law enforcement personnel required under § 1542.217(c)(2), if applicable.	(3) Training program for law enforcement personnel required under § 1542.217(c)(2), if applicable.
(12) A description of law enforcement support used to comply with § 1542.215(a).	(2) A description of the law enforcement support used to comply with § 1542.215(a).	(2) A description of the law enforcement support used to comply with § 1542.215(b).
(13) A system for maintaining the records described in § 1542.221.	(4) A system for maintaining the records described in § 1542.221.	(4) A system for maintaining the records described in § 1542.221.
(14) The procedures and a description of facilities and equipment used to support TSA inspection of individuals and property, and aircraft operator or foreign air carrier screening functions of parts 1544 and 1546 of this chapter.	X	X
(15) A contingency plan required under § 1542.301.	(5) The contingency plan required under § 1542.301.	X
(16) Procedures for the distribution, storage, and disposal of security programs, Security Directives,	(6) Procedures for the distribution, storage, and disposal of security programs, Security Directives,	(5) Procedures for the distribution, storage, and disposal of security programs, Security Directives,

Complete	Supporting	Partial
Information Circulars, implementing instructions, and, as appropriate, classified information.	Information Circulars, implementing instructions, and, as appropriate, classified information.	Information Circulars, implementing instructions, and, as appropriate, classified information.
(17) Procedures for posting of public advisories as specified in § 1542.305.	(7) Procedures for public advisories as specified in § 1542.305.	(6) Procedures for public advisories as specified in § 1542.305.
(18) Incident management procedures used to comply with § 1542.307.	(8) Incident management procedures used to comply with § 1542.307.	(7) Incident management procedures used to comply with § 1542.307.
(19) Alternate security procedures, if any, that the airport operator intends to use in the event of natural disasters, and other emergency or unusual conditions.	X	X
(20) Each exclusive area agreement as specified in § 1542.111.	X	X
(21) Each airport tenant security program as specified in § 1542.113.	X	X

Also, under 1542.103 (d) Use of appendices, the airport operator may comply with paragraphs (a), (b), and (c) of this section by including in its security program, as an appendix, any document that contains the information required by paragraphs (a), (b), and (c) of this section. The appendix must be referenced in the corresponding section(s) of the security program.

Note the significant difference between the Complete and the Supporting and Partial Security Program requirements. Supporting and Partial programs do not have airside security requirements, such as Secured Area, AOA, or SIDA. Without these requirements, several other elements are also not generally required, such as credentialing (i.e., providing access or identification media), escorting authorized personnel who do not possess approved media but do have approved access provided they are under escort, and challenging those without approved media. Also, one difference between a Supporting and a Partial program is that a Partial program is not required to have Contingency Plans.

Key Takeaways

1. The type of security program is based on the airport's category, related to the number of annual passenger enplanements received at that airport compared to the annual number of enplanements from all commercial service airports throughout the nation, and the nature of its flight operations.
2. The majority of commercial service airports in the US have Complete security programs.
3. Supporting and Partial security programs typically do not have airside security areas.

2.1.1 Changing Airport Security Programs

ASCs who must implement a higher security program (e.g., move from Partial to Supporting or Complete) should compare the existing requirements to the new requirements from Table 2-1 and implement new procedures as necessary. ASCs should work closely with TSA and other airport operators with higher level security programs. ASCs may require higher levels of security access to the

Homeland Security Information Network (available through TSA application) to receive the materials necessary to implement the increased security measures.

ASCs should assess the new security requirements thoroughly to understand their scope and implications, and identify the staff members and tenants who will be affected by these requirements; ASCs should also prepare clear, concise training and communication materials that outline the new procedures. Furthermore, ASCs should schedule meetings with all affected personnel and companies, focusing on those entities that will be most affected; distribute written materials summarizing the new security requirements; encourage feedback; and conduct operational readiness and testing on the new systems prior to full implementation.

2.2 Airport Security Coordinator Roles and Responsibilities

The most critical position in the administration of the ASP is that of the ASC. ASC roles are assigned with a Primary ASC and typically at least one Alternate ASC (and sometimes as many as ten Alternate ASCs). Although the responsibilities related to carrying out the requirements of 49 CFR § 1542 are the same for both the Primary ASC and the Alternate ASC, assigned duties tend to vary widely depending on the airport's size and organizational structure. The assignment of duties and the number of Alternate ASCs designated for each airport can have a significant impact on the effectiveness of the ASP, and ultimately the effectiveness of the airport's overall security posture.[6]

As specified in Part 1542 – Airport Security, the TSA requires that the airport designate one or more ASCs for the ASP and that they perform the six security functions noted below:

1542.3 Airport Security Coordinator

- Serve as the primary and immediate contact for security related activities and communications with the TSA.
- Be available on a 24-hour basis.
- Frequently review security functions to ensure compliance with the ASP, and applicable Security Directives.
- Immediately initiate corrective action for any instance of non-compliance with the ASP or applicable Security Directives.
- Review and control the results of employment history, verification, and criminal history records checks.
- Serve as the contact to receive notification from individuals applying for unescorted access of their intent to seek correction of their criminal history record with the FBI.

2.2.1 Primary ASC

An airport will have only one Primary ASC identified in the ASP, with this individual being the primary point of contact for TSA. The Primary ASC is responsible for the content and implementation of the ASP, and establishing how many Alternate ASCs will be designated and their roles and responsibilities.

An airport's size, complexity, and management style will dictate the Primary ASC's roles and responsibilities. Typical assignments and responsibilities for the Primary ASC at different airport categories include:

[6] TSA-NA-03-02 Airport Security Coordinator Training Curriculum

- **Category X & I –** The largest and most complex airports uniformly assign this role to senior-level security managers, who then typically delegate most of the day-to-day duties to Alternate ASCs.
- **Category II & III –** Mid-sized airports often assign this role to the Director of Operations and/or Security who performs the day-to-day administration of the program. Often Alternate ASCs will be assigned secondary duties, such as being responsible for ASP amendments or badging office duties, to lessen the operational burden on the Primary ASC.
- **Category IV –** The smallest airports almost exclusively use the airport manager as the Primary ASC, and as such that individual performs all the duties required in the ASP, often with significant assistance from an Alternate ASC.

At one Category III airport that was interviewed, the Chief of Police is designated as the Primary ASC and is responsible for the duties in the ASP and other administrative functions.

The organizational profiles shown above represent the industry standards. These management structures have proven over the long term to be effective in implementing the requirements of the ASP and are accepted by TSA.

Occasionally, airport leaders may re-assign Primary ASC duties to positions that would normally occupy an Alternate ASC role. This break in the chain of command can lead to miscommunications, blurred lines of responsibilities, and ultimately security issues that have the potential to require corrective action from TSA. As such, these decisions should be carefully considered.

Key Takeaways

1. An ASP designates only one individual as the Primary ASC, and they are the first point of contact for TSA.
2. The Primary ASC has the ultimate responsibility for the effectiveness of an ASP.
3. Following the chain of command is important when assigning the role of Primary ASC to a position.

2.2.2 Alternate ASCs

The Primary ASC will determine the number of Alternate ASCs needed to meet the requirements set forth in 49 CFR § 1542.3, with assigned duties tending to vary depending on the airport's management structure and security category. Typical assignments and responsibilities for Alternate ASC are shown below:

- **Category X & I –** The largest and most complex airports vary widely from using only one to as many as ten Alternate ASCs. Most airports in this category use three or four, with certain positions performing the bulk of the day-to-day security management duties. Typically they serve in key positions such as Vice President of Security, Assistant Security Manager, or Operations Security Manager. Additional Alternate ASCs are often put in place to provide the 24/7 on-call requirements of 49 CFR § 1542, and be able to initiate immediate action for any security incident.
- **Category II & III –** Mid-sized airports normally range from two to four Alternate ASCs. They provide support for a variety of administrative work, such as ASP amendments and airport badging duties. Additionally, they are used to fulfill the 24/7 availability requirement.

- **Category IV –** The smallest airports almost always have only one or two Alternate ASCs. But at the smallest commercial service airports, these positions often take on roles like that of their large commercial service airports counterparts. It was noted they were routinely assigned a significant role in administering ASP duties. This is attributable to the minimal staffing levels at small airports and the wide diversity of duties for which personnel at small airports are responsible.

Many factors should be considered when determining the number of Alternate ASCs to assign in the ASP. Airports assigning too many Alternate ASCs is a concern of TSA regulatory managers. TSA officials have noted that when the number of Alternate ASCs at an airport exceeds four, a variety of issues can arise, including:

- Lack of consistency in addressing security issues
- Communication gaps amongst ASCs
- Internal notification issues
- Lack of experience in dealing with security issues

Key Takeaways

1. An airport is not limited to a certain number of Alternate ASCs.
2. Duties and responsibilities assigned vary widely among airports, with Alternate ASCs often playing senior leadership roles in day-to-day security operations.
3. TSA officials recommend airports designate a minimal number of Alternate ASCs to help reduce a variety of potential issues.

2.2.3 Operational Considerations for ASC Duties and Responsibilities

Fundamentally, the ASC is the linchpin of the ASP and their responsibilities are wide-ranging. All airport ASCs and alternates must have their names published in the current version of the ASP, and at least one individual trained and designated as an ASC must be available to TSA on a 24/7/365 basis.

The Primary ASC must possess an in-depth knowledge of aviation security, airport operations, and aircraft operations to understand the impact of security measures to those operations. To that end, ASCs should also familiarize themselves with other relevant Federal Aviation Regulations (FAR) and CFRs, including FAR § 139 Airport Certification, CFR § 1544 Aircraft Operator, CFR § 1546 Foreign Aircraft Operator, CFR § 1548 Indirect Aircraft Operator, and CFR § 1550 Aircraft Operator Security Under General Operating Rules. Appendix A contains additional resource documents for ASCs.

Part 1542.3(b)(3) requires ASCs to "review with sufficient frequency all security-related functions to ensure that all are effective and in compliance with this part, its security program, and applicable Security Directives." Practically speaking, this statement involves the ASC drafting the ASP, disseminating information from SDs and amendments, creating amendments for construction, and resolving other related changes to airport security such as changed conditions. A changed condition means a condition on the airport that is inconsistent with what is described in the ASP, and may require immediate action to correct and notification to the TSA. ASCs must also ensure law-enforcement response to checkpoints and security breaches of restricted areas, including the Secured and Sterile Areas. Additionally, ASCs are integral in negotiating Exclusive Area Agreements (EAA) and Airport Tenant Security Program (ATSP) agreements.

"Security-related functions," also include, to a certain extent, passenger checkpoint operations. Although the ASC is not responsible for passenger screening, they may still be involved with the screening process, such as the creation of procedures to allow non-passengers through the checkpoint. The ASC participates in checkpoint operations in the event of a security breach into the Sterile Area, and when the screening checkpoints are closed, the checkpoint itself becomes a Part 1542.207 access point for which the airport operator is responsible. The ASC also has a certain level of control over access to the Sterile Area by airport workers through Part 1542.207 access control points, and is responsible for implementing airport worker inspection and screening programs.[7] ASCs play an important part in planning and designing or redesigning security checkpoints, access control and credentialing systems, and Federal Inspection Stations. ASCs should also maintain liaison with airline Station Managers and Ground Security Coordinators.

Per 1542.3(c), all ASCs must complete subject-matter training as specified in its ASP prior to assuming the duties of the position. In certain cases, TSA might allow an ASC to be temporarily appointed and trained by another ASC or prior ASC, with the commitment to complete a formal program of study within a certain timeframe. Once trained as an ASC and listed in the ASP, the Primary or Alternate ASC will have access to SSI materials, such as SDs and NAs. They should be reviewed immediately upon completing ASC training.

Per 1542.3(d), once ASC training has been completed, the ASC does not have to undergo retraining unless there has been a two-year break in service as an active and designated ASC. The regulations do not address whether an Alternate ASC qualifies under this regulation, and it might be at the discretion of TSA to determine whether an individual must retrain as an ASC. The ASC training curriculum is available to airport operators from TSA; many trade associations, universities and private companies also provide ASC training.

2.2.4 Airport Consortium

The development of an ASP should be a group effort, as the security regulations apply to and affect airport operators, tenants and other users. Additionally, many of the responsibilities of the ASC are often performed by other entities, such as airport police, airport operations personnel, airport security, etc. Therefore, ASCs should consider establishing and maintaining an Airport Security Consortium. The airport operator should clearly define the structure and scope of authority of the Consortium.

In addition to the ASC, consortium membership could include members of the airport law enforcement agency, TSA, FBI, US Customs and Border Patrol, US Immigration and Customs Enforcement, airport project management, airport operations, air traffic control, airport security, ARFF personnel, emergency medical personnel, the US Postal Service, and any off-airport entities with authorities or responsibilities under the ASP.

At some point in the process, the ASC should include representation from the airport's legal department, particularly when making changes to the ASP or addressing any TSA-related complaints or issues.

[7] TSA-NA-23-02 Aviation Worker Screening

Key Takeaways

1. The ASC is the cornerstone of the ASP who is responsible for managing numerous elements of the airport's security program.
2. An ASC's responsibilities are far more extensive and complex than what is articulated in the CFRs.
3. ASCs should be just as familiar with airport and aircraft operations as they are with aviation security processes and principles.

SECTION 3: DEVELOPING ASP CONTENT

The table of contents (TOC) for an ASP typically follows the regulatory structure and sequence of Part 1542. The sequence used in this section also forms a natural table of contents should the reader desire to use it. Many airport operators follow the TOC format from the TSA, which reflects the sequence of CFR § 1542, but some may use a different TOC structure, with TSA approval.

The ASP must be marked as SSI as specified CFR § 1520.13 Marking SSI. The ASP should also be clearly marked as the "Airport Security Program" on the front cover. Each page should also include a stamp for the Federal Security Director's signature, a line for the date signed, and a notation saying, "TSA Approved," (or similar wording).

A submittal page should be included with the term "Submitted By," (or similar) along with the printed name, title of the airport management designee (e.g., airport director, CEO, ASC), and a signature line and date line, along with an "Approved By" (or similar) and the printed name and title of the TSA approving official, and a signature and date line.

This can be followed by a TOC and a Record of Amendments. From an administrative perspective it may be easier to include the Record of Amendments prior to the TOC as amendment pages may be added from time to time. An Abbreviations and Definitions section should also be included. Most of the necessary definitions for an ASP can be found in CFR § 1540.5 "Terms used in this Subchapter." Additional information on formatting content can be found in Section 5.1.3.

When generating a new ASP, or updating sections of the existing ASP, TSA may require the integration of existing SDs, and TSA local and NAs. A list of currently applicable NAs, SDs, and other documents is included in Appendix A. A checklist for creating an ASP is included as Appendix E.

3.1 Purpose of the ASP

This section of the ASP describes the purpose of the document as noted in Part 1542.101(a)1. The overall purpose of the ASP is to explain how the airport operator will carry out all related security requirements under CFR § 1542 and other applicable regulations.

Sample language for the Purpose of the ASP

This ASP is submitted in compliance with 49 Code of Federal Regulations (CFR), Chapter XII, Part 1542. The measures contained in this Airport Security Program (ASP) must be complied with in accordance with 49 Code of Federal Regulations (49 CFR), Transportation Security Regulations, section 1542.101(a). The airport operator must ensure that the measures contained in this ASP are implemented to provide for the security of persons and property on an aircraft operating in air transportation against an act of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary onto an aircraft.

3.2 Airport Description

The Airport Description can include the airport's approximate location in reference to the central business district; its location in the city and county; a description of the facility including the number commercial service terminal buildings and their sizes in square feet; and an overview of other facilities, particularly those where screening may also be occasionally or always conducted (such as a Fixed-Base Operator or Charter Operator), and whose flight operations may be under an aircraft operator security program. The official airport mailing address should also be included.

In some cases, the ASC may include the airport's category in the section (Cat X, I, II, III or IV).

3.3 Airport Ownership

The Airport Ownership paragraph explains the FAA-recognized airport sponsor (i.e., owner of the airport). A line of succession is also frequently included.

3.4 Responsibilities of ASCs and Alternate ASCs

This section of the ASP should identify the ASC and their responsibilities, along with the responsibilities of any alternate ASCs, and a record of Primary ASC and Alternate ASC training requirements.

3.5 ASC Contact Information

The ASP should list the name and contact information of the Primary ASC, and the names and contact information of any Assistant, Alternate, or Associate ASCs. With TSA approval, the airport operator can provide TSA with a central point-of-contact number, such as an Airport Operations Center, who can immediately get in touch with the on-call ASC.

3.6 ASC Training Requirements

Training records for ASCs and alternate ASCs must be maintained until 180 days past the time where the ASC (or alternate) no longer is serving in that capacity.[8,9]

3.7 Other Necessary Information

The ASP can also include anything else the airport operator feels is necessary. However, airports should remember that anything in the ASP is subject to regulatory enforcement by the TSA. In some cases, airport operators may decide to write the ASP to the regulatory minimum, but operationally exceed the ASP standards.

Key Takeaways

1. The ASP must be approved by TSA and marked as SSI.
2. The airport description, ownership, and other relevant administrative information should be included in the ASP.
3. The responsibilities of the ASC are outlined in the ASP.
4. The ASP can be written to the regulatory minimum, but that does not restrict the airport from operationally exceeding the ASP standards.

3.8 Security Areas and Access Control Systems

Parts 1542.201 through 1542.207 address three security areas within the Complete Security Program: the Secured Area, the AOA and the SIDA. The Sterile Area is referenced in Part 1542.211(b) and defined in Part 1540.5. Each area mandates certain security procedures the airport operator must

[8] Local record retention schedules may call for retaining records for a longer period of time.
[9] TSA-NA-03-02 Airport Security Coordinator Training Curriculum

implement. These protocols primarily address access control systems; personnel identification; and the systems, measures, and procedures for regulating access and verifying an individual's authorization to be within a security area. Most of the security area access and identification requirements address airport workers, but the Sterile Area addresses access by passengers and others with authorized approval.[10]

NOTE: For ASCs with prior industry experience, this section may be particularly confusing as many airports will use different terms to describe the security areas.[11] However, in SDs, NAs, ICs, and other documents, TSA uses these specific terms. For example, it is important to know that a Secured Area and a SIDA have two distinct definitions. ASCs may have to "translate" previous terminology in use at their airport to TSA's definitions.

3.8.1 Security of the AOA

It should be noted that the definition of an AOA within the security domain is different from the definition of an AOA commonly used to describe aircraft operational areas. From an operational perspective, the AOA includes the runways, taxiways, and ramp areas where aircraft operate. From a security perspective, an AOA may include *certain* runways, taxiways and ramp areas, but not all of them. Some AOAs may include a SIDA, or an airfield area may be designated a Secured Area, in which case that area adopts the Secured Area access control requirements and the term AOA (from a security perspective) is dropped altogether. There is no such designation as a Secured Area/AOA – it is either one or the other, as each has specific access control requirements.

Airport operators operating under Part 1542.103 (i.e., the Complete Security Program) are required to establish an AOA that must **prevent** and **detect** the unauthorized entry, presence, and movement of individuals and ground vehicles into or within the AOA. The airport operator must establish and carry out measures for controlling entry to the AOA in accordance with Part 1542.207(c), which requires the airport to incorporate accountability measures. The term "accountability measures" is broad and can have a variety of applications.

There are several methods of implementing an access control system for an AOA that integrates accountability measures, such as:

- A Fixed-Base Operator, charter company, or large aircraft operator with its own hangar and/or terminal facilities, might use its personnel to monitor and allow access to authorized personnel to their ramp area, or install their own physical access control system. It is common for such operations to allow access to pilots operating general aviation aircraft and escorting their passengers to and from the aircraft.
- A security gate that opens when presented with AOA-only access media. The access control system should record who the card is issued to, and the time of entry.
- A physical lock and key with a list of authorized users on file with the airport operator. This is common for small general aviation hangar areas.
- Maintaining a key log for physical keys issued to airport tenants in the general aviation areas.

[10] These are commonly authorized visitors, parents accompanying traveling minors to the gate, and caretakers assisting elderly or those with disabilities.

[11] For example, it is common for ASCs to call the Secured Area the SIDA, as employees can often better recognize the meaning of that term, whereas within the ASP the SIDA actually meets the requirement of a Secured Area. It is also common to use the term "Restricted Area," on signs leading into the Secured Area, Sterile Area, SIDA, or AOA as the general public better understands the term "Restricted Area," than the regulatory language.

Personnel based at the airport who only operate in the AOA are required to undergo an Security Threat Assessment (STA) and possess airport-approved identification. In consideration of federal requirements, the airport operator must determine whether the credential check and identification display requirements of the SIDA should also apply to AOA-based personnel (i.e., do personnel in the AOA have to display access identification?).

AOA-based personnel do not have to undergo security training (unlike those operating in a Secured Area or SIDA), but must be provided with security information as required under Part 1542.213(c). This includes information on unescorted access authority of the individual to enter and be present in various areas of the airport; control, use, and display of airport-approved access and identification media, if appropriate; escort and challenge procedures, and law enforcement support for these procedures, where applicable; security responsibilities as specified in Part 1540.105 (Security Responsibilities Of Employees and Other Persons); restrictions on divulging SSI as described in Part 1520; and any other topics specified in the security program.

In constructing a security program, it may be advantageous to first establish the boundaries of the AOA, as illustrated in Figure 3-1, before layering additional levels of security such as the SIDA and Secured Area.

Key Takeaways

1. The minimum security layer on the airfield is the AOA.
2. Access control requirements within the AOA must incorporate accountability measures.
3. Personnel based at the airport who only operate in the AOA are required to undergo an STA, be issued airport-approved identification (that restricts access to just the AOA), and receive security information.
4. It is important to note that operational and security-related descriptions of the AOA may vary, and it is important to clearly define AOA boundaries for security purposes to avoid confusion.

Figure 3-1. Example of an AOA

Source: Leading Edge Strategies

3.8.2 Security of the SIDA

Under 1542.205, airport operators with a Complete Security Program must establish at least one SIDA. A SIDA is an area where individuals must wear an airport-approved identification credential, such as an airport identification media, airline identification, or other approved identification. Airport operators must establish and carry out measures to prevent the unauthorized presence and movement of individuals in the SIDA, and establish a personnel identification system (under Part 1542.211), subject each individual to a criminal history record check and STA (under Part 1542.209), and train each individual before granting access to the SIDA (under Part 1542.213[b]). Airports with a Supporting or Partial Security Program are not required to establish a SIDA.

A true—by definition—SIDA does not have access control requirements. The SIDA assumes or adopts access control requirements when combined with an AOA or Secured Area. SIDAs by themselves (i.e., without access control requirements) are most commonly found inside airline cargo facilities, whereas AOA/SIDAs are found on air cargo ramp areas. Also, Secured Areas must meet the requirements of a SIDA, but have additional access control requirements beyond that of the AOA.[12]

Cargo facilities, including vehicle docks and areas where an aircraft operator, foreign air carrier, or indirect air carrier sorts, stores, stages, consolidates, processes, screens, or transfers cargo must be designated a SIDA. Publicly accessible vehicle dock areas are often separated from the SIDA by using a visible deterrent such as a marking on the pavement or a stanchion with retractable belts. Access by unauthorized individuals is hindered as everyone in the SIDA with unescorted access is required to challenge and report anyone without the proper identification.

The part of the AOA where cargo is loaded or unloaded from an aircraft that is operated in a Full or Full All-Cargo security program, or a foreign air carrier (conducting cargo operations), must be a SIDA.

Figure 3-2. Example of a SIDA

Source: Leading Edge Strategies

[12] Note: The access control requirements for an AOA are less than the requirements for entry into a Secured Area.

Key Takeaways

1. A SIDA is an area where approved identification media must be displayed.
2. A SIDA, in and of itself, does not have access control requirements, but adopts any access control requirements of an AOA or Secured Area.
3. An example of a SIDA without access control requirements is in the airline cargo facilities where the public area and SIDA are often distinguished by a marking on the floor.

3.8.3 The Secured Area

The Secured Area represents one of the highest levels of security on the airport. Secured Areas are established around domestic and foreign scheduled passenger operations, and in areas where checked bags are screened and sorted. The Secured Area extends until stopped by an approved barrier. Approved barriers might be buildings, fences, the runway/taxiway system (i.e., the Movement Area), waterways, time-and-distance, or an electronic barrier.[13] At many airport access points, the Secured Area is protected through a card reader and door alarm system that is connected to the Physical Access Control System (PACS). It is a best security practice to limit the amount of access points to the fewest possible.

Each commercial service airport operating under Part 1542.103 (i.e., a Complete Security Program) must establish at least one Secured Area under Part 1542.201 and carry out access control measures that provide for detection of and response to each unauthorized presence or movement in, or attempted entry to, the Secured Area by an individual whose access is not authorized in accordance with the ASP. Secured Area boundaries must be described in the ASP along with any barriers used to separate the Secured Area from other security areas and the public area.

Secured Areas essentially replace the AOA, in terms of required security measures. Per Part 1542.207, Secured Area access controls must ensure only those who are authorized to have access can access the Secured Area, deny access to those without access authority, and differentiate access authority between individuals who have access to one point in a Secured Area but not others. The Secured Area also requires a personnel identification system that meets the requirements of a SIDA.

Within the Secured Area, the system must verify that the holder of the identification media is entitled to pass through the portal and either unlock it to allow passage or deny passage (if access is unauthorized). Under Part 1542.203(a)(2), airports are required to have a response to each unauthorized presence or movement in, or attempted entry to the Secured Area. The type of response is not specified in the regulations. Subject to TSA approval, response options may include using audible and/or visual alarms (i.e., flashing lights) on doors that access Secured Areas to alert nearby personnel, or door alarms that electronically notify an operations center whereupon a security officer, LEO, or other employee can be dispatched to investigate the source of the alarm. Another option may be to use a two-way audio/video system, whereby operations center staff can conduct a visual check of the door area and talk to individuals at that location via an intercom. At some airports, certain tenants or air carriers may be responsible for response to door and gate alarms, instead of the airport operator.[14,15]

[13] At present, TSA does not have an "approved," electronic barrier, but notes they will consider airport-proposed electronic barriers on a case-by-case basis.
[14] This is often dependent upon whether the airline has an Exclusive Area Agreement, or a tenant has an Airport Tenant Security Program.
[15] TSA-NA-12-04 Response to SIDA Door Alarms

If is determined that a breach has occurred, airport security and/or law enforcement personnel should be notified and a search for the individual should be conducted. If the search is unsuccessful, airport authorities should, in consultation with TSA, decide on the next steps (i.e., stop flight operations until it can be determined a breach did not actually occur, the individual causing the breach is found, or the situation is reconciled in some other way).

Access to the Secured Area should be logged at the time of entry. For vehicle access, entry should only be provided through a staffed access gate. This enables security personnel to conduct any required or recommended security inspection of the vehicle, and to ensure its occupants are all authorized or under proper escort to enter the Secured Area. Vehicles should also exit the Secured Area through a staffed exit gate. These regulations may not apply in certain cases, such as for airport law enforcement, firefighter personnel, airport operations, and airport maintenance personnel who may access and exit the Secured Area through unstaffed access points.

Access to the Secured Area does not necessarily have to be controlled by the PACS. The same objectives might be attained by stationing a security officer (or individual with similar authority) at an access point. This officer should be provided with a radio with direct communications to a centralized security or airport operations center. They can make a radio or cell phone call to the operations center to verify the access authority of each individual desiring access through the access point. By using the Stop List, the individual can also prevent unauthorized access. The officer should also be issued a Stop List that includes a list of airport identification badges that have been invalidated in the credentialing system, but the physical badge has not been returned to the airport operator and has not expired.

Some airport operators have elected to make the entire airfield a Secured Area. However, while potentially providing a higher level of security, this option may not be affordable for some airports or tenants, as they would have to implement more comprehensive and expensive access control systems throughout the entire facility. Some airport operators find it more affordable and practical to designate only the area around commercial service aircraft as a Secured Area, as shown in Figure 3-3.

Figure 3-3. Example of a Secured Area

Source: Leading Edge Strategies

Key Takeaways

1. Airports are required to establish a Secured Area around air carrier operations and areas where bags are loaded and sorted.
2. A Secured Area must meet the requirements of a SIDA, plus add access controls that can authorize access, deny access and differentiate access between security areas and public areas.
3. The airport operator must carry out access control measures that provide for detection of, and response to, each unauthorized presence or movement in, or attempted entry to, the Secured Area.

3.8.4 The Sterile Area

Sterile Area security is only addressed in Part 1542 in relation to its dimensions and the access controls used when the checkpoint is not in operation. It is also addressed in Part 1540.5 and the aircraft operator regulations Parts 1544.201 and 1546.201. All regulations should be reviewed when considering procedures for establishing and maintaining the security requirements of the Sterile Area.

CFR §§ 1544 and 1546 address the requirements of domestic and foreign aircraft operators, but since both the aircraft operator and the airport operator control access to the Sterile Area, the air carrier regulatory requirements are noted in Part 1544.201 Acceptance and screening of individuals and accessible property.[16]

Part 1540.7 states that no individual may enter a Sterile Area or board an aircraft without submitting to the screening and inspection of their person and property in accordance with the present access control procedures. However, these processes do not specifically require all persons to undergo the passenger screening process. There are exceptions and alternatives as described below.

Airport operators must determine who will be allowed access to the Sterile Area through the checkpoint and how that access is provided. Access to the Sterile Area is generally restricted to passengers with a valid boarding pass and, in certain cases, authorized visitors such as parents accompanying minors to the gate, and caretakers assisting elderly individuals or persons with disabilities.

Access to the Sterile Area is commonly provided by two primary methods: through the screening checkpoint, and through Part 1542.207 airport-controlled access points. A Part 1542.207 access point meets the access control requirements of a Secured Area (i.e., allow access, deny access and differentiate access authority), and is typically used by airport workers to transition from the Secured to the Sterile Area and back. The ASP must note any access points that access a Sterile Area.

Additionally, the airport operator must establish procedures to ensure adherence to Secure Flight (1540.107[a][2]), which addresses personnel who need access to the Sterile Area but are not boarding an aircraft (usually airport workers). Airport operators must consider how they will gather the necessary information to fulfill the requirements of this section. Airports include the necessary information required by Secure Flight in their airport worker access/identification badge application so when the application is approved, the worker has already been vetted through Secure Flight.[17]

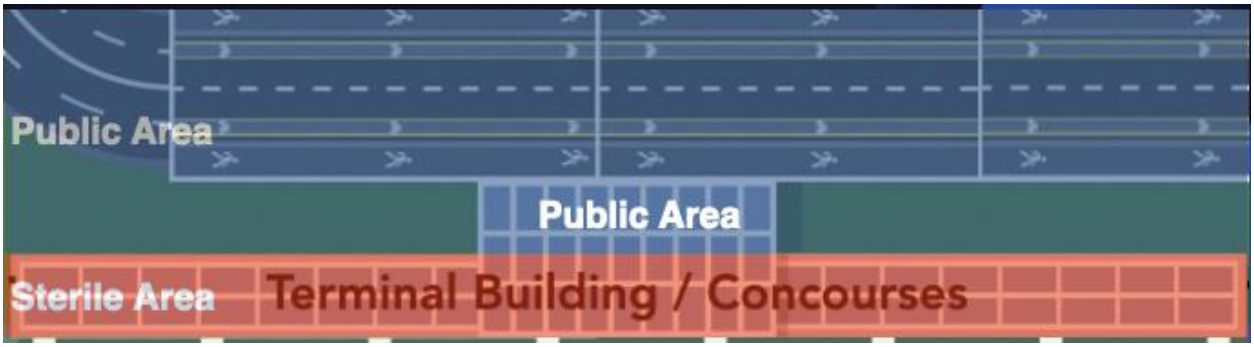
Part 1542.211(e) Escorting (5) addresses individuals accessing the Sterile Area without unescorted access authority. Airport operators should consider processes to escort individuals who have not undergone the passenger screening process into the Sterile Area. This may include escort conducted by

[16] The foreign air carrier regulations under TSR Part 1546.201 are similar to the domestic regulations.
[17] TSA-NA-23-02 Aviation Worker Screening

an individual with (a) unescorted access authority and (b) who has authorization to conduct an escort, and (c) accompanies that individual the entire time they are in the Sterile Area. Some airports have added a visitor badge process whereby such individuals are provided a badge to be worn while in the Sterile Area (unescorted or escorted). Airport operators should determine whether an individual who has submitted to the passenger screening process must still be escorted. The ASC should refer to Part 1542.211 (e)(5), which states, "Ensure that individuals escorted into a Sterile Area without being screened under § 1544.201 of this chapter remain under escort until they exit the sterile area or submit to screening pursuant to § 1544.201 or § 1546.201 of this chapter."

Air carrier personnel access requirements into the Sterile Area and on board an aircraft is addressed in air carrier–related policies and permissions from TSA. Whether air carrier employees can access an aircraft or Sterile Area through a Part 1542.207 access control point and then board an aircraft or be present in the Sterile Area without first undergoing the passenger screening process is a question for TSA and air carriers who may have guidance on this process. Airport operators should consult with the air carrier Station Managers or Ground Security Coordinators to clarify this policy.[18,19]

Figure 3-4. Example of Sterile Area



Source: Leading Edge Strategies

3.8.5 Protection of the Exit Lane

Protection of the exit lane can be the responsibility of the airport operator or TSA, depending on circumstances and local policies. The airport operator must demonstrate how the exit lane is protected and provide procedures for the passage of law enforcement personnel and others authorized to bypass the screening checkpoint. The exit lane might be protected through the use of security personnel, through authorized technologies or other means as approved by TSA. Consult with the FSD for proper guidance, and reference PARAS 0023 *Exit Lane Strategies and Technology Applications,* for additional information on exit lane protection.

Key Takeaways

1. Sterile Areas are the part of an airport defined in the ASP that provides passengers access to boarding aircraft, and to which the access generally is controlled by TSA or aircraft operators.
2. Airport operators are responsible for access to the Sterile Area when checkpoint operations are closed, and for Part 1542 access control points.

[18] It should be noted that airline crew members who are not based at a particular airport, routinely access the screening checkpoint via the Known Crewmember program. Airline crew members based at a particular airport may have airport-issued access identification depending on the airport's policies.
[19] SD 1542-04-10 Airport Tenant Access to the Sterile Area

3. Individuals who do not undergo the passenger screening process but have a need to be in the Sterile Area must be under escort by an individual with unescorted access authority.

3.8.6 Access Control Systems

Commercial service airports often employ intricate access control systems designed to cater to a diverse workforce (e.g., tenants, vendors, air carriers, LEOs) that ranges from a few dozen to upwards of 50,000 airport workers, each possessing varying levels of access privileges. These systems may be interconnected with CCTV systems and incorporate alarm systems, airport identification badges and/or biometric or PIN authentication.[20] It is imperative that these access control systems satisfy both the operational demands of the airport and the stringent federal regulatory mandates at all times. The Radio Technical Commission on Aeronautics publishes the *Standards for Airport Access Control Systems*, which provides guidance on the integration of access control systems into an airport, along with other information on identity management, perimeter intrusion detection, security operations center and communications, and biometrics.

Access control systems are based on authentication: "something you know" – like a PIN code, "something you have" – i.e., an airport identification badge, and/or "something you are" – i.e., biometrics. Airport operators select at least one of these methods to control access; some may incorporate two or all three methods. Once an individual's personal information is authenticated, the system allows passage through a door or gate.

Airport operators must determine what methods will be used to control access to the Secured Area in a way that authorizes personnel with access authority, denies access to those without access authority, and can differentiate authorized access from one access point to another (as addressed in Section 3.10.3). Operators must also consider how they will control access to the AOA in a way that incorporates accountability measures (as addressed in Section 3.10.1).

Part 1542.207(a) addresses the access control requirements for Secured Area access. A basic access control system uses single-factor authentication, which is typically the airport ID media. The ID media is often issued by the airport operator after the credentialing process has been successfully completed. The badge is then encrypted with an embedded code that is unique to that individual. The code is read by a card reader through proximity or card swipe, which then allows access to the access point. Additional methods of access control can include the use of PIN codes and biometrics. Airport operators must also determine how non-based airline personnel (i.e., those without airport-issued identification media) can access airline operational areas. The use of PINs and biometrics may be beneficial in these instances.

Part 1542.207(b) addresses alternative systems an airport operator may implement (with TSA approval) where a Secured Area standard access control system cannot be used. This may be airfield markings, signage, constant surveillance by CCTV or security personnel, or other means.

Part 1542.207(c) addresses AOA access. The airport must determine what accountability measures will be taken to ensure unauthorized personnel are prevented access into the AOA and from the AOA to higher levels security on the airfield.

[20] PIN – Personal Identification Number

Part 1542.207(d) addresses secondary access media. This may be issued to an individual who already has unescorted access authority to the Secured or AOA but is temporarily not in possession of their ID media. This regulation allows the airport operator to temporarily issue a secondary access media (such as another identification badge). The airport operator must determine whether this measure will be allowed at the airport and the processes for issuing the media. The disadvantage of issuing additional access media is the increase in the number of issued access media that airport operator must account for during the audit process.

Vehicle access and movement is addressed in both Parts 1542.201(b) and 1542.203(b). Airport operators are required to prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into and within the Secured Area and AOA. Access control requirements for the Secured Area are higher than for the AOA, so a variety of methods may be used. Airport operators should consider how to identify authorized vehicles (e.g., stickers/decals, signs), the procedure for issuing vehicle permits and, if necessary, how to search vehicles entering the security areas.

Key Takeaways

1. Airport operators must determine how to control access to security areas.
2. Access requirements for the Secured Area are different than for the AOA.
3. Secondary access media may be issued at the discretion of the airport operator.

3.8.7 Barriers

Although not specified in the regulations, airport operators often use a combination of barriers to ensure the integrity of the security areas and fulfill the access control requirements. Some suggestions for barriers may include physical (walls, buildings, fences), natural (waterways, time and distance), access points (gates and doors) and electronic (laser sensing or similar technologies).

Physical barriers in airport security include structures such as the terminal buildings and various types of fences, with the airport perimeter fence being a notable example. Fencing is a common choice for airport perimeter protection. Fencing comes in various designs, incorporating features that make it challenging to climb or breach. More advanced systems utilize motion sensors, tension systems, or other electronic monitoring methods. Typical airport considerations include the type of fencing or walls, whether any sort of barbed or razor wire will be used, and whether the fencing will be sunk into the ground to prevent tunneling.

Airport operators must also consider how far apart to place warning signage on the airfield barriers to deter entry into the security areas. The distance between signs may depend on the nature of air carrier operations and the airport’s geographical characteristics (e.g., an airport located in a city may need more frequent signs).

Within the terminal, physical barrier considerations include whether interior walls will extend beyond the false ceiling.

Access points are entryways such as doors and gates designed for personnel and vehicle access. From a security practices perspective the airport operator may categorize access points based on their operational purpose: routine, maintenance, or emergency. Routine operations gates are utilized by a wide range of personnel needing daily access to the airfield, such as vendor delivery staff, airline ground-service equipment operators, maintenance personnel, operational staff, and non-emergency response police personnel. These locations typically have high levels of activity. Maintenance entry

points are utilized by maintenance personnel and provide access to electrical rooms, heating, ventilation and air conditioning areas, plumbing, etc. Emergency access points often include doors with crash bars, which allow emergency egress but alarm upon activation. Airport operators should determine how doors or gates that are used for emergency purposes provide a notification to the airport operators, (i.e., audible, visual, and/or electronic notification to an operations center). There are a variety of vehicle access gates available to airport operators. PARAS 0028 *Recommended Security Guidelines for Airport Planning, Design and Construction* provides an excellent resource for airport perimeter fencing and gates.

Natural barriers can include bodies of water, swampland, or cliffs. The term "natural" does not necessarily mean created by nature. Some natural barriers are intentionally constructed, like human-made lakes. Natural barriers can also include functional obstacles, such as time-and-distance. This is the concept of situating assets so that it will take an intruder a considerable amount of time to traverse the distance to reach them, providing an opportunity for someone to detect and respond to the intrusion.

Perimeter intrusion detection systems are another consideration for perimeter protection. A variety of technologies can be considered, such as laser fencing, motion sensing, etc.

Key Takeaways

1. Barriers are often used to control access to and between the security areas of the airfield.
2. In addition to standard physical barriers, additional levels of security may be reached through the use of perimeter intrusion detection systems.
3. Natural barriers can be both physical, such as a lake or ocean, or the concept of time-and-distance, which can be used to deter intrusions and provide time respond to attempts to enter security areas.

3.9 Fingerprint-Based Criminal History Record Checks and Security Threat Assessments

The basic credentialing process consists of an application, which includes a request from the applicant employer's Authorized Signatory,[21] a background check comprising at a minimum a fingerprint-based Criminal History Record Check (CHRC) and a Security Threat Assessment (STA), training the airport worker on use of the badge and any other security requirements as called for in the regulations, and any other security information as determined by the airport operator, and then, upon final approval from the ASC, issuance of the badge. The airport operator must determine how to categorize the Authorized Signatory personnel and how many individuals from each company can be an Authorized Signatory.

There have been numerous changes to the fingerprint-based CHRC and STA process as outlined in Part 1542.209, so the airport operator must work closely with TSA and check all relevant SDs and NAs related to this process. Regulatory citations in Part 1542.209 that reference 14 CFR § 107 refer to pre-9/11 FAA security regulations that no longer exist.[22]

[21] The Authorized Signatory serves as the official representative of an airport tenant, air carrier, contractor, vendor, or government agency. Authorized Signatories are responsible for requesting airport access/ID and requesting access levels for their company or government entity's employees. The ASC retains the ultimate decision-making authority when it comes to granting ID badges or access privileges. Authorized Signatories also serve as the primary point of contact to the ASC on security matters. (TSA-NA-18-03 Authorized Signatory)

[22] Post 9/11/01, Title 14 CFR § 107 was changed to address small unmanned aircraft systems.

Airport operators must establish procedures to issue credentials to personnel authorized to be in the SIDA—what is known as "unescorted access authority." Part 1540.5 states that:

> *Unescorted access authority* means the authority granted by an airport operator, an aircraft operator, foreign air carrier, or airport tenant under Part 1542, 1544, or 1546 of this chapter, to individuals to gain entry to, and be present without an escort in, secured areas and SIDA's of airports.

The ASP must thoroughly explain the procedures used to comply with the CHRC/STA process. These procedures outline the steps for an applicant who desires an access ID with unescorted access authority to a SIDA, Secured Area, or Sterile Area. The airport operator must collect, control, and process at least one set of legible and classifiable fingerprints for the CHRC, and information for the STA check. Further, airport operators must establish a badge application process that collects disclosures of any disqualifying offenses and information necessary to complete the STA (under Part 1540.201), determines the applicant's level of access authority, and is signed (electronically or otherwise) by an Authorized Signatory. Part 1542.209(e) addresses requirements that must be on the airport badging application. The airport operator is also required to verify the identity of the applicant. Some airport operators post the credentialing procedures online along with the forms used in the badging and access control application process.[23]

Any applicant that has been convicted of any of the 28 disqualifying offenses, or has been found not guilty by reason of insanity of any of the 28, within the last ten years (Part 1542.209(d)) cannot be issued unescorted access identification. The airport operator must also have procedures in place for those whose CHRCs are returned noting an arrest but without a disposition. The procedures must cover notifying the applicant of their status, and the requirements to demonstrate that the disposition did not result in a conviction of one of the 28 disqualifying offenses. Under Rap Back, the FBI will notify airport operators of any badge holder that has been arrested or subsequently convicted of a crime. However, procedures must also be developed for current badge holders to notify the airport operator if they have been convicted (or found not guilty by reason of insanity) after having access/identification issued.

Once the fingerprints and information for the STA have been collected, the airport operator sends them to a Designated Aviation Channeler, who collects the appropriate fees, and works with the FBI and TSA to process the CHRC and STA.

Airport operators must determine if individuals without unescorted access authority can be escorted while in the SIDA, Secured Area, or Sterile Area while they are awaiting the results of their credentialing check.

In certain cases, a certification form may be used instead of a badge application. A certification form informs the airport operator that a CHRC has already been completed. This form may be used for air carrier personnel, government employees, or other individuals who have undergone the CHRC as part of their employment process, and can provide their FBI Fingerprint Identification Number to the airport badging office.[24]

---

[23] SD 1542-04-08 STA and Reports; TSA-NA-21-03 Criminal History Records Checks (CHRC) and the Federal Bureau of Investigation (FBI) Rap Back Program; TSA-NA-19-02 Airport Identification Media Audits; TSA-NA-18-01 Airport Access and Vetting; TSA-NA-21-01 Centralized Revocation Database for Individuals with Revoked Identification Media.

[24] Airport operators often create separate application forms for individuals who have already completed the CHRC. Examples of these forms can be found on many airport websites.

The airport operator must have procedures in place for individuals who are continuously employed, meaning they have had an access/identification previously issued to them by the airport operator and are applying for a badge to work for another company at the airport. This often happens when an individual leaves employment with one company at the airport and switches to employment with another company at the airport. Each airport operator must determine the maximum duration between employment dates that meets the definition of continuously employed.

Airport operators must also identify which personnel are Trusted Agents. Trusted Agents hold distinct responsibilities outlined by DHS and are tasked with handling airport worker badge applications, gathering data for STAs, and overseeing the fingerprinting process for CHRCs. ASCs must provide the names of all Trusted Agent to the FSD, and each Trusted Agent must also pass a CHRC and STA.

Key Takeaways

1. Each individual requiring unescorted access authority to a security area must successfully complete a credentialing process that includes a fingerprint-based CHRC and an STA.
2. It is the airport operator's responsibility to verify the identification of the badge applicant, collect a set of classifiable fingerprints, and collect the information necessary to conduct the STA.
3. Trusted Agents are tasked with processing the applications for airport worker CHRCs and STAs.
4. The Rap Back program administered by the FBI will notify airport operators of any badge holder who has been arrested or subsequently convicted of a crime after the initial background checks have occurred.

3.10 Personnel Identification Systems

3.10.1 Airport Identification Badges

Airport identification badges must follow Part 1542.211. The ID media must:

- Show a full-face image, name, employer and unique identification number
- Indicate, to the extent possible, the scope of the individual's access and movement privileges
- Clearly indicate clearly an expiration date
- Be of sufficient size and appearance as to be readily observable for challenge purposes

The airport operator must determine the size of the ID media. Historically, airport badges are three inches by five inches in size and can have a vertical or a horizontal orientation. The badge's indication of access and movement privileges may be done through a variety of methods such as the badge color, a background image, icons displayed on the badge, or a combination of these.

The airport operator is required to establish protocols for retrieving expired ID media, reporting instances of lost or stolen media, and securing unissued identification stock and supplies. It is mandatory for the airport to conduct an annual audit to verify the integrity of the identification system. In cases where an unacceptable percentage of issued, unexpired media is lost, stolen, or unaccounted for, the operator must reissue all airport badges. Some airport operators issues fines or charge higher fees for replacing lost ID media.

3.10.2 Temporary Access Identification

Temporary ID media are issued for temporary personnel. Airport operators must have procedures to authorize the use of temporary identification media, retrieve temporary ID media, and ensure that

temporary ID media are distinct from other identification media and meet the requirements of Part 1542.207(d) Secondary Identification Media.

There are situations when the airport operator may approve alternate forms of identification for use in security areas, such as for FAA Flight Standards District personnel, TSA inspectors, or air carrier personnel. Airport operators must generate procedures and rules for determining who has the ability to use non-airport-issued identification credentials.

Reference the Radio Technical Commission on Aeronautics: Standards for Airport Access Control Systems for more information on constructing a personnel identification and access control system.

3.10.3 Escorting and Challenging

Escorting is the act of an authorized individual accompanying an individual who does not possess the proper identification into a security area. Under Part 1542.211(e) Escorting, it is the responsibility of the airport operator to determine who has the privilege of escorting other individuals who do not have access authority to security areas.

Part 1542.211(d) notes that individuals under escort are to be continuously accompanied and monitored while in the Secured Area or SIDA in a manner sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted, and to act in accordance with the ASP.

Note that the regulations do not specify the number of individuals a person with unescorted access authority can escort. Airport operators must answer this question and define the escort procedures appropriate for their airports operating characteristics. Escorting, both personnel escorts and vehicle escorts, is widely understood as accompanying to a point where they are in visual contact and under verbal control of the unescorted individual. The purpose is to regulate the actions and mobility of the escorted persons or vehicles and to respond appropriately in case of unauthorized activity or movement.

Challenging is the act of an authorized individual asking to see another individual's access media when that person's access media is not visibly displayed or in their possession when in a SIDA. Under Part1542.211(d) Challenge Program, it is the airport operator's responsibility to determine challenge procedures for their employee with unescorted access authority.

Airport operators must explain the requirements of the challenge program, answering questions such as "who is required to challenge," and explain the procedures an employee with unescorted access authority must follow, when encountering an individual that cannot produce the appropriate access identification media in a security area. Airport operators must also establish the rules for escorting individuals who do not have unescorted access authority.

Key Takeaways

1. Airport operators must establish a personnel identification system that identifies individuals with unescorted access authority in the Secured Area and SIDA.
2. There are certain personnel identification such as FAA or air carrier personnel the airport operator can approve for use in the Secured Area or SIDA.
3. Airport operators must establish rules for challenging individuals in a Secured Area or SIDA that are not in possession of the proper access identification.

3.10.4 Training

Under Part 1542.213 Training, individuals operating in the SIDA or Secured Areas are required to undergo training in their security-related functions, as specified in the ASP and relevant NAs, SDs, and ICs. Training topics may include but are not limited to:

- The rules and responsibilities related to having unescorted access authority
- Control, use, and display of ID media
- Escorting and challenge procedures
- Law enforcement notification
- Restrictions on divulging SSI
- Other airport security rules and regulations as specified in the ASP

Airport operators must establish the training procedures for individuals with unescorted access authority. Some airports, especially smaller ones, provide in-person training in a classroom setting. Others have decided that computer-based training is more efficient, particularly when training dozens of people on a daily basis.

Note that individuals who have access to the AOA, or Sterile Area privileges and access the Sterile Area through the security checkpoint, do not have to undergo security training, but must be provided with security information. The information is similar to the Secured Area and SIDA training programs. The regulations do not specify how this training information is to be distributed, or how new tenants and employees working in the AOA are to receive new or updated information.

Key Takeaways

1. Personnel with unescorted access authority in the Secured Area or SIDA must complete security training.
2. Personnel should be trained in the security responsibilities including the responsibilities of having unescorted access authority.
3. Individuals within the AOA are not required to receive security training but must be provided with security information.

3.11 Law Enforcement Support

In accordance with Part 1542.217, each airport operator required to have a Complete or Supporting Security Program must provide uniformed law enforcement personnel:

- In a number and manner adequate to support its ASP, and each system for screening persons and accessible property required under Part 1544 or 1546
- Who are available and committed to respond to an incident in support of a civil aviation security program when requested by an aircraft operator or foreign air carrier that has a security program under Part 1544 or 1546
- Who are able to respond to issues at the screening checkpoint and other acts of unlawful interference
- Who have arrest authority, are trained and sworn as a peace officer, are in uniform or other indicia of authority, and are armed with a firearm

There is not a specific number of LEOs required for each airport category. It is up to the airport operator, with TSA approval, to determine the adequate number of LEOs necessary to support the ASP.[25]

Each airport that is required to have a Partial Security Program under Part 1542.103(c) must ensure that the procedures to request law enforcement support are provided to each aircraft operator or foreign air carrier that has a security program under Part 1544 or 1546. Airport operators must explain how these requirements will be met.

In certain cases, an airport operator may not have an adequate number of LEOs available to support the ASP. Under Part 1542.219 Supplementing Law Enforcement Personnel, TSA may enter into an agreement with the airport operator to use, on a reimbursable basis, personnel employed by TSA, or by another department, agency, or instrumentality of the government, with the consent of that agency.

3.11.1 Recordkeeping

Part 1542.221 Records of Law Enforcement Response, requires records related to law enforcement actions to be retained for 180 days.[26] Records are required to be kept for:

- Weapons, explosives, or incendiaries discovered at the screening checkpoint
- Any acts of air piracy (hijacking, commandeering), bomb threats, real or simulated bombs, and actual detonations
- The number and types of arrests, including the identifying information of each arrested individual and, if applicable, the aircraft operator on which the individual was arrested or was scheduled to be a passenger on

The nature of how these records must be retained must be explained to in the ASP, and the records must be made available for TSA inspection upon request.[27]

Key Takeaways

1. Airport operators must have enough LEO personnel to address the requirements of the ASP and support response to the screening checkpoints and acts of unlawful interference on an aircraft.
2. In certain cases, airports may not have adequate available LEO personnel, in which case they may qualify for TSA's supplementing law enforcement program.
3. The airport operator must retain certain records related to LEO response for a minimum of 180 days.

3.12 Contingency Measures, SDs, ICs, Public Advisories, and Incident Management

3.12.1 Contingency Plan

Part 1542.301 Contingency Plan mandates that airports be capable of responding to federal government requests for an elevation in their security posture. The airport must conduct reviews and exercises of the plans and ensure all parties involved with each plan understand the responsibilities. Alternate procedures

[25] TSA-NA-11-01 Patrols
[26] Note: Local record retention requirements may extend this time period.
[27] SD 1542-04-08 STA and Reports

may be approved by TSA provided they ensure an overall level of security equal to the contingency plan. Airport operators must draft the contingency plans and include them in their ASP.

3.12.2 Security Directives and Information /Circulars

Part 1542.303 Security Directives and Information Circulars states that TSA may issue an IC to notify airport operators of security concerns. When TSA determines that additional security measures are necessary to respond to a threat assessment or to a specific threat, TSA issues an SD that sets forth mandatory measures, requiring airport operators to develop procedures for the timely receipt, dissemination, and implementation of SDs, or to propose alternative measures to TSA.

SDs and ICs are considered SSI and can only be distributed to those with an operational need to know under Part 1520. The airport operator must determine a method by which to disseminate the information within an SD or IC to only those with a need to know.

TSA has recently transferred many previous SDs to NAs.

3.12.3 Public Advisories

When advised by TSA, each airport operator must prominently display and maintain in public areas information concerning foreign airports that, in the judgment of the Secretary of Transportation, do not maintain and administer effective security measures. This information must be posted in the manner specified in the security program and for the duration determined by the Secretary of Transportation.[28]

3.12.4 Incident Management

Part 1542.307 Incident Management requires the airport operator to establish procedures to evaluate bomb threats, threats of sabotage, aircraft piracy, and other unlawful interference with civil aviation operations. Airport operators must determine how to evaluate each threat, respond in accordance with the Airport Emergency Plan, and notify TSA of the incident.

Key Takeaways

1. Contingency plans must be outlined in the ASP.
2. Airport operators must comply with SDs and only issue SD information to those with a need to know.
3. Incident management procedures must be outlined in the ASP and in accordance with procedures in the Airport Emergency Plan.

3.13 Exclusive Area Agreements and Airport Tenant Security Programs

3.13.1 Exclusive Area Agreements

Section 1542.111 Exclusive Area Agreements are amendments to the ASP under which an aircraft operator or foreign air carrier that has a security program under Part 1544 or 1546 assumes responsibility for specified security measures for all or portions of the Secured Area, AOA, or SIDA, including access portals. EAAs are commonly used for airline hangars and other facilities, such as

[28] TSA-NA-23-01 Public Advisories

airline flight planning and administrative office areas, where the aircraft operator will assume certain functions that are normally the responsibility of the airport operator.

EAAs must contain a description, a map and, where appropriate, a diagram of the boundaries and pertinent features of each area, including access portals, personnel identification media, or other measures. The EAA must describe the security measures employed by the aircraft operator or foreign air carrier to adhere to the relevant sections, namely the Secured Area, AOA, or SIDA. The only portion of the ASP an aircraft operator cannot accept responsibility for is law enforcement response. EAAs must be in writing, signed by the airport operator and aircraft operator or foreign air carrier, and maintained in the ASP.

The assumption of responsibility must be exclusive to one aircraft operator or foreign air carrier. Shared responsibility among aircraft operators or foreign air carriers is not permitted for an Exclusive Area. Airport operators must identify which air carriers desire EAAs and the security measures for which the air carrier will accept responsibility, and any amendment or changed notification process. Each EAA must be signed by the airport operator, TSA, and the air carrier.

Figure 3-5. Example of Exclusive Area

Source: Leading Edge Strategies

3.13.2 Airport Tenant Security Programs

Part §1542.113 Airport Tenant Security Programs are amendments to the ASP under which an airport tenant that is not an aircraft operator accepts responsibility for certain airport security measures provided in the Secured Area, AOA, or SIDA. ATSPs are similar to EAAs but are used by non-regulated entities, which are not regulated under Part 1544 or 1546.

ATSPs must be in writing, signed by the airport operator, the tenant, and TSA, and become part of the ASP. The requirements of an ATSP are similar to an EAA except the airport operator must provide

systems, measures, or procedures for monitoring and auditing the tenant's compliance with the ATSP, whereas TSA primarily enforces EAA compliance.

Figure 3-6. Example of Airport Tenant Security Program Area

Source: Leading Edge Strategies

Key Takeaways

1. EAAs and ATSPs are agreements between the air carrier or an airport tenant, the airport operator and the TSA, whereby the air carrier or tenant assumes certain airport security responsibilities.
2. EAAs are exclusive to air carriers regulated under Part 1544 (domestic aircraft operator) or Part 1546 (foreign air carrier).
3. ATSPs required the airport to monitor tenant compliance with the ATSP.

3.14 Inspection Authority

Part 1542.5(c) grants TSA the authority to be "at any time or place," including security areas, with or without ID media issued or approved by an airport or aircraft operator, in order to conduct inspections related to the ASP. For this reason, many airport operators include an example of the TSA Inspector credential in their ASP, and write into the ASP that the credential is approved for access to security areas. In this way the airport operator can better distinguish a TSA Inspector from a threat actor. It is not uncommon for visiting TSA Inspectors (i.e., not based at the airport) to conduct tests of the ASP as local Inspectors will often become known to security and law enforcement personnel at their airport.

TSA can also require the airport to issue their personnel airport access or identification media to provide unescorted access to Secured Areas, AOAs, and SIDAs. However, such personnel are required to complete the airport SIDA training.

Key Takeaways

1. TSA personnel have the authority to inspect the ASP, be in security areas, and inspect security-related records, with or without airport- or airline-issued access or ID media.
2. TSA's authority extends to being in and on airport areas to inspect for compliance with aircraft operator security programs.
3. TSA may require the airport operator to issue ID media to TSA personnel, but only after those personnel have completed the airport SIDA training.

3.15 Airport Enforcement of the ASP

Although not specifically addressed in the regulations, airports are expected to enforce the requirements of the ASP as it relates to airport workers. Enforcement of the ASP related to the general public is commonly carried out by law enforcement personnel (e.g., respond to breaches, respond to alarms). ASP enforcement on airport workers typically involves enforcing security-related rules and regulations, ensuring they are wearing their identification badge, not propping doors open, etc.

Part of this enforcement process is disseminating portions of the ASP into the airport's Rules and Regulations. The airport operator should work with TSA to determine which parts of the ASP can be publicly disseminated in the form of the Rules and Regulations, and which ones are to remain solely in the SIDA training program. The Rules and Regulations should address violations by airport workers such as loaning their ID media, improper use of their ID media, leaving security area access portals opened and unstaffed, etc. The ASP should also describe the consequences of such violations, such as a violation notice, mandatory retraining, or suspension or revocation of their ID media.

Key Takeaways

1. Airports must enforce the requirements of the ASP.
2. Airport should work with TSA on the Rules and Regulations to determine which parts of the ASP can be publicly disseminated.

3.16 Cybersecurity

To defend and protect against cybersecurity threats, airport operators are required to:

- Report significant cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency
- Establish a cybersecurity point of contact
- Develop and adopt a cybersecurity incident response plan
- Complete a cybersecurity vulnerability assessment
- Develop an approved implementation plan that describes measures the airport is taking to improve their cybersecurity resilience and prevent disruption and degradation to their infrastructure
- Proactively assess the effectiveness of these measures, which include the following actions:
    a. Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an information technology system has been compromised, and vice versa

b. Create access control measures to secure and prevent unauthorized access to critical cyber systems
c. Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operations
d. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on critical cyber systems in a timely manner using a risk-based methodology[29,30]

[29] TSA. (2023, March 7). *TSA issues new cybersecurity requirements for airport and aircraft operators | Transportation Security Administration*. TSA. https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft
[30] TSA-NA-21-05 Cybersecurity Incident Reporting; TSA-NA-22-01 Cybersecurity Self-Assessments and Incident Response Plans; Emergency Amendment (EA) Joint EA 23-01 Cybersecurity – Performance-Based Measures; Cybersecurity Requirements for United States Airport Fueling Operations.

SECTION 4: IMPLEMENTING ADMINISTRATIVE CHANGES

The aviation industry is ever changing, so airport operators may be required to change their ASP. ASPs are typically changed through a permanent or temporary amendment, which can be initiated by the airport, TSA, an SD, an NA, or a notice of a changed condition that affects security. This section describes what causes ASP amendments and provides guidance for efficient amendment submissions and reviews by the TSA. Recommendations are provided to help simplify TSA approval processes and ensure SSI materials are protected.

4.1 Amendment Types

There are several ways an ASP can be amended. Some are required by the TSA and others by the airport operator.

INFORMATION CIRCULAR (IC)

TSA may issue an IC to notify airports of security concerns. An IC is for informational purposes only and is not a mandatory requirement. This is simply a notification stating security concerns that the airport operator shall be informed about, a need-to-know basis.

SECURITY DIRECTIVE (SD)

TSA issues an SD when it determines that further security actions are needed to respond to a threat assessment or known threat against aviation. An SD is mandatory, and airports must comply with its stated security measures. Under Part 1542.303 each airport must comply with each SD issued to the airport within the timeframe specified in the directive. When an airport receives an SD, they must:

- Verbally acknowledge that they received the SD
- Explain how the airport will comply with the SD
- If the airport is unable to comply with the security measures in the SD, they must submit to TSA for approval the alternative measures they plan to take

EMERGENCY AMENDMENT (EA)

TSA can issue an EA when there is an emergency that requires immediate action with respect to safety and security in public transportation. TSA does not have to give prior notice for comments or reviews by the airport as it must be implemented within the specified timeframe. An airport can appeal the EA but must comply with the requirements while the appeal process is underway.

NATIONAL AMENDMENT (NA)

TSA can issue NAs to security programs that affect all applicable airport operators. NAs may have review and implementation periods whereby industry has an opportunity to provide feedback before the amendment is finalized.

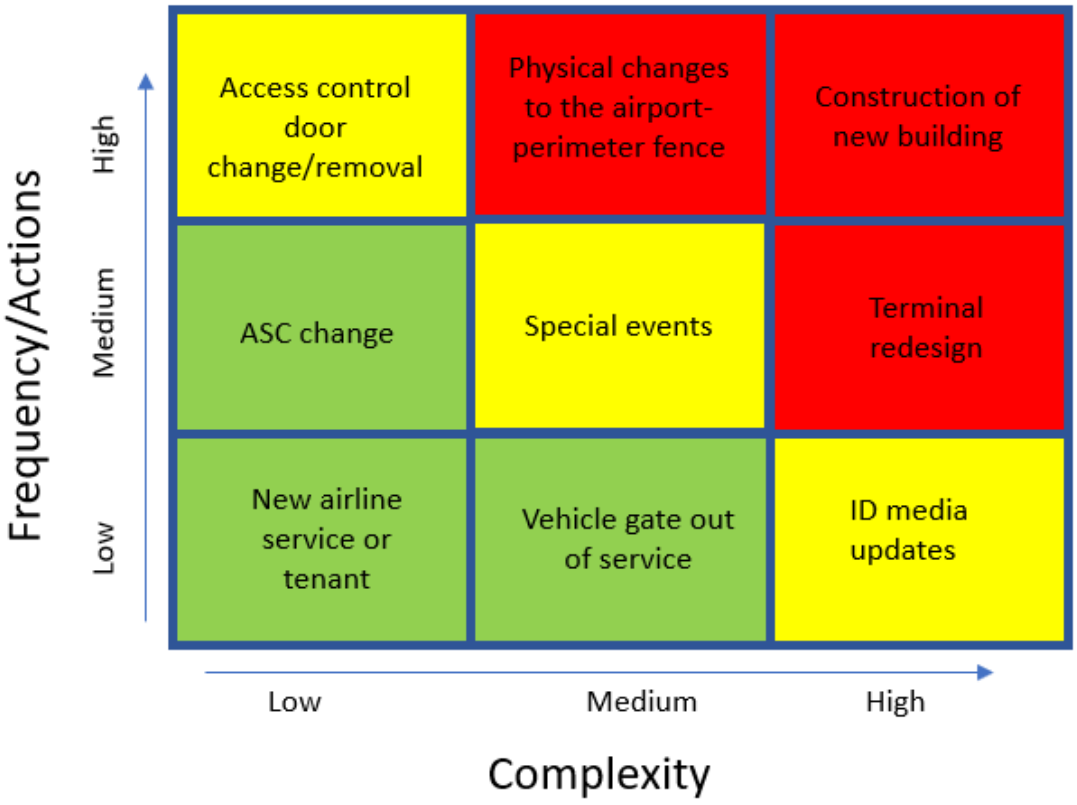
CHANGED CONDITION

A changed condition occurs when some condition on the airport changes, causing a different condition than what is described in the ASP. For example, an access control door may change or go out of service, a vehicle gate may break, or a new building may be constructed. When a temporary condition cannot be maintained to the extent described in the ASP, a changed condition occurs. The airport must notify the TSA within 6 hours of the change, and a written notification must be submitted within 72 hours. If the changed condition is expected to continue past 60 days, the ASC must submit an amendment to TSA within 30 days.

The level of impact that a temporary or permanent amendment will have on an airport will depend on the changes that need to occur in order to maintain an equivalent level of security to the facility and the duration of the corresponding event. If the changed condition results in a permanent physical change to the facility, changes to layouts and procedures described in the ASP will typically be required.

Several airports surveyed were completing major terminal construction projects and stated that temporary amendments were routine for facilitating the construction needs and for showing building modifications. Other reasons for changed condition amendments included personnel changes, required testing, recurrent training, annual exercises or special events, construction, new airline service or tenants and any physical changes to the airport. Figure 3-1 below shows the most common amendment types and their level of operational impacts to the ASP based on frequency and complexity.

Figure 4-1. Amendment Type – Impact Assessment Matrix



Key Takeaways

1. An SD is a mandatory requirement and airports must comply with their security measures.
2. TSA can issue emergency amendments to security programs when there is an emergency that requires immediate action with respect to safety and security in public transportation.
3. A changed condition occurs when some condition on the airport changes that causes a different condition than what is described in the ASP.

4.2 Submission Process

Submitting changes to the ASP typically involves the Primary ASC drafting the work and submitting it to local TSA for approval. The Alternate ASC has authority to submit changes to TSA, but most often the Primary ASC heads the task.

The following five steps outline the basic amendment process:

1. Initial communication between TSA and airport on the upcoming amendment
2. Verbal agreement on the amendment language and intent
3. Airport sends a draft version to TSA for review and comment
4. TSA comments are incorporated into the draft amendment
5. The draft amendment is submitted to TSA for review and approval

Final review and approval are conducted by the FSD. Once the amendment has been approved, it is sent back to the airport for inclusion in the ASP, procedural changes are applied, and those changes are then communicated to the appropriate stakeholders.

One major challenge discussed during the interviews was that amendment language often goes through several draft submittals to TSA before a final approval is made, thus delaying the approval process significantly. Clear communication with TSA on the front end of the amendment process to explain the intent and provide a description of the amendment would likely reduce delays in the final approval process.

The majority of airports surveyed submit their changes through a password-protected email. Other submission options include the use of a web-based platform such as SharePoint. One airport uses a closed network standalone computer system that the TSA is able to access—essentially a shared drive with a shared firewall. However, most airports are not currently doing this as TSA is not typically on site at their airport. Finding ways to increase collaboration and share documents through faster avenues may be a way for airports to streamline the submission process.

Other options for submitting changes to TSA include the use of data encryption software (e.g., VIRTRU, Bit Warden). If an airport is interested in utilizing the software to send changes to TSA, local TSA will need to seek approval from headquarters as an alternate means for password-protected documents.

Key Takeaways

1. Submitting changes to the ASP typically involves the primary ASC drafting the work and submitting it for approval.
2. Final review approval is provided by the FSD.
3. Other options for submitting changes to TSA include the use of data encryption software,

4.3 Information Dissemination

The method used to disseminate security information is directly related to the type of information and its intended audience. When changes to the ASP require coordination and communication with stakeholders, ASCs typically deliver the information via emails with password-protected documents and/or security meetings. Some airports utilize a document-sharing portal with login credentials for Authorized Signatories where the ASC can send information to specific groups, such as airlines or

concessionaires. This is a quick and convenient method for airports to get information out in a timely manner.

Data encryption software discussed in the previous section allows the user to send out information to a specific set of recipients with certain controls, such as allowing the recipient to read the information but not print it. Other options include text messages that point to where to find and review the amendment, security bulletins, and security meetings where specific stakeholders are informed of the changes.

The method of communication to be used will vary based on the size of the airport and the time sensitivity of the information that is being provided.

Key Takeaways

1. The method used to disseminate security information is directly related to the type of information and its intended audience.
2. Some airports utilize a document-sharing portal with login credentials for Authorized Signatories where the ASC can send information to specific groups, such as airlines or concessionaires.
3. Data encryption software allows the user to send out information to a specific set of recipients with controls.

4.4 Effective Protection of SSI Amendments

Effective protection of SSI documents is crucial to the protection of the ASP. SSI is information that if publicly released would be harmful to transportation security. The most widely used method for protecting SSI material is saving it in an electronic format with password protection. Smaller airports interviewed used a PDF protected with the current standard TSA password. Larger airports used Microsoft SharePoint files with several layers of security protections. One Cat X airport interviewed utilized an official TSA email that was provided by TSA to the airport specifically for ASP updates.

Larger airports were able to utilize several more technologically advanced methods for SSI protection because they have more firewalls, and often TSA resides at the airport, allowing them to share documents within the airport's network.

Key Takeaways

1. Effective protection of SSI documents is crucial to the protection of the ASP.
2. The most widely used method for protecting SSI material is saving it in an electronic format with password protection.

SECTION 5: PROGRAM MAINTENANCE STRATEGIES

This section expands on ways to ensure the ASP is regularly maintained, and considerations for the secure storage of program documents. Each section provides practical guidance and key takeaways for ASCs to use as they implement the day-to-day tasks of their ASP.

5.1 Routine Program Maintenance

Once the airport has established a comprehensive TSA-approved ASP and is able to effectively disseminate security information, the task of routine program maintenance takes center stage. A well-maintained ASP will be current and free from obsolete or incomplete information. Equally important is ensuring that all the working copies are fully reflective of the master copy. Additionally, properly formatting the ASP will ensure it is easy to amend, with minimal formatting changes required in the document during minor amendments. The task of maintaining the document is paralleled with the ongoing responsibility to store and protect SSI information from unauthorized access.

One of the most important aspects of maintaining the ASP is ensuring that each working copy of the ASP is secured and is the most up to date version. Establishing the required minimum number of copies, in addition to the master copy, will assist in this task. This number will be based on the size and complexity of the airport and the number of alternate ASCs that have been assigned to the program. Most Cat X–III airports maintain two or three hard copies for use in the badging office, command center, and other operationally focused areas. Cat IV airports typically just have a master copy located securely in the manager's office that is accessible by both the Primary and Alternate ASCs. As airports move to electronic-only versions of the ASP, the issue of storage and maintaining up-to-date versions of working copies will dissipate.

A Cat I airport reported that they maintain 16 hard copies of their ASP, in addition to the master copy. This has proven to be an ongoing administrative burden and exposes the airport to unnecessary security risks related to protecting SSI.

The following sections will help guide ASCs in the routine maintenance of their ASP.

5.1.1 Developing a Review Program

The development of a comprehensive review program will ensure that the ASP and any secondary copies of the ASP are always up to date and maintained in a secure manner. Consistency and redundancy in the review process will ensure that the ASP is being reviewed and updated in accordance with the requirements of current TSA directives and airport security needs.

The ability to quickly locate regulatory information in the ASP will assist airport security managers in their ability to effectively verify the information in ASP for initial, routine, and amendment-related reviews. This task can be streamlined with the creation of a standalone document that identifies regulatory requirements and lists the corresponding pages in the ASP that contain that information. The Regulatory Reference document can be created by the ASC or used in conjunction with the Checklist for reviewing the ASP located in Table 5-2, below. A working copy is in Appendix E.

Although the review methods may vary by airport, one example would be for the Primary ASC to oversee the process and assign a limited number of alternate ASCs to perform and document the reviews. The primary ASC would routinely review the records and coordinate with the alternate ASCs.

The frequency and scope of ASP reviews will be dependent on the airport's security category as well as any local conditions that would affect the contents of the ASP. Typically, airports that have a higher security category will experience an increased frequency of conditions or security procedures that require changes to the ASP. Furthermore, airports that are experiencing high levels of construction activity, security issues, or personnel changes are likely to need amendments and ASP reviews with increased frequency. There are several different amendment types that can be further broken down into routine or significant amendments as discussed below.

ROUTINE AMENDMENTS

Routine amendments to the ASP are caused by a variety of events that include:

- Temporary construction
- Personnel changes
- Administrative changes
- Temporary access points/security area changes
- Airline service/tenant changes
- Procedural changes
- Temporary security procedure/special events
- Access media/technology changes

One leading reason for temporary amendments to the ASP is construction activity that alters physical layouts, access points, and security procedures. These tend to have estimated time frames for each construction phase, which result in frequent updates and amendments to the ASP as the project progresses from one phase to the next. Routine amendments may also require other sections of the ASP to be amended; this should be considered during each ASP amendment request to the TSA.

SIGNIFICANT AMENDMENTS

Significant amendments in the ASP tend to be initiated by TSA guidance or a condition that results in a change that has overlapping implications in the ASP. These can include the following:

- Permanent construction
- Permanent airfield/building modifications
- Permanent access points/security area changes
- New TSA guidance/security procedures

Completed projects will normally result in new building or airfield layouts that require amendments to security procedures in the ASP. As these changes are updated and approved in the ASP, other sections of the document such as diagrams and related procedures may become obsolete, resulting in additional amendments. Checklists to assist in the review process are provided in Tables 5-1 and 5-2. A working copy of Table 5-2 is in Appendix E.

Table 5-1. Recommended Frequency of Airport Security Program Reviews & Checklist

Airport Category	3-Month	6-Month	12-Month	After Significant Changes
X	P	C	—	C
I	P	C	—	C
II	—	P	C	C
III	—	P	C	C
IV	—	P	C	C

P - Partial Review C – Complete Review (See Review Checklist)

Table 5-2. Checklist for Reviewing the ASP

#	Description of Content 1542.103	Reviewed Current (c) or Not Current (nc)	Regulatory Reference Page (s)	Resolved Date
1.	**Contact Information**			
2.	Blank			
3.	**Secured Areas**			
4.	**AOA Areas**			
5.	**SIDA Areas**			
6.	**Sterile Areas**			
7.	**Procedures for CHRC**			
8.	**Personnel ID systems**			
9.	**Escort Procedures**			
10.	**Challenge Procedures**			
11.	**Training Programs**			
12.	Law Enforcement Support			
13.	Record Maintenance			
14.	**Screening Procedures**			
15.	Contingency Plan			
16.	SSI Dissemination			
17.	**Posting Public Advisories**			
18.	Incident Management Procedures			
19.	Alternate Security Procedures			
20.	Exclusive Area Agreements			
21.	Airport Tenant Security Programs			
22.	**Review compliance with all current EAs, NAs, and ICs**			

***Bold sections should be completed during Partial Reviews**
***A working checklist is provided in Appendix E**

Key Takeaways

1. Establishing a consistent review system is critical to maintain a current ASP.
2. At a minimum, the ASP should be reviewed every six months or when significant changes occur at the airport.
3. Construction projects are the leading cause of ASP updates, both temporary and permanent.

5.1.2 Streamlining Content & Minimizing Revisions

The content in each section of the ASP should be complete, detailed, and presented in a logical sequence. The use of appendices with maps, charts, and drawings to complement written descriptions is an effective tool for streamlining and simplifying complicated sections. This is particularly relevant in the sections where Secured, AOA, SIDA, and Sterile Areas are described. Appendices are also often used to detail personnel identification systems, security procedures, public advisory postings, Airport Emergency Plan (from Airport Certification Manual), EAAs, and ATSPs.

While the goal of each section is to be complete and accurate, at times the information provided needs to be more general due to the size and complexity of the airport. Sections should primarily list content that has a direct operational impact on security. Airports should work closely with their TSA counterparts to agree on the extent of the ASP content. Many large and complex airports focus on access points and other high-risk areas in their detailed drawings, with large-scale overviews of other low risk areas. This approach not only simplifies the ASP's format, but also streamlines the process of creating construction amendments, and minimizes any final updates in the ASP after significant construction projects are completed.

Airports varied in the level of detail they included in their ASP. ASCs stated that they prefer to use a detailed description in each section of the ASP that is clear and concise to meet, not exceed, the intent of the regulation. Occasionally, due to a specific condition or previous occurrence, TSA will require an airport to exceed the normal standard and requires that additional language be included in the ASP regarding an additional security procedure or as an upgrade to minimum physical requirements.

Important considerations are noted below:

- ASCs should maintain an ASP that meets, but does not exceed, the requirements established by TSA regulations and directives.
- Exceeding TSA regulations can strengthen the security posture of one area of an airport, but it can also place increased duties and responsibilities on staff.
- Care should be taken when voluntarily exceeding the TSA requirements, and a thorough cost-benefit analysis should be performed prior to the inclusion of additional language in the ASP.

Another often overlooked aspect of the content in the ASP is the use of generic verbiage to reduce the frequency of routine administrative amendments. For example, the use of position titles instead of individual names, and the use of generic numbering of door and gate locations will help eliminate the need for administrative amendments due to personnel or tenant turnover.

Larger airports may consider implementing a Content Management System (CMS) or Governance, Risk, and Compliance (GRC) platform to manage their ASP revisions. These tools can enable efficient management of content, correlation of information, and automated auditing capabilities.

Key Takeaways

1. Content must be sufficiently detailed and presented in a logical manner.
2. Maximize the use of appendices with maps, etc. to reduce written descriptions and to simplify the document.
3. Reduce the need for revisions by using generic verbiage when possible.
4. Only include additional language in the ASP that exceed TSA requirements if the benefits outweigh the costs.

5.1.3 Formatting Content

Word processing software that allows user-friendly editing, strong password protections, and compatibility with other document formats is essential for efficient ASP management. A number of commercially available options are available for airports to use, with most airports reporting the use of Microsoft Word for editing documents and Portable Document Format (PDF) being used for final document viewing.

The ability to perform efficient and streamlined editing of an ASP relies on the ability to only change a limited section of the document and avoid format disruptions throughout the entire document. Although at times this type of document content shift is unavoidable due to the size or specific nature of the amendment, the following steps can be taken to simplify the editing process:

- Airports maintaining hard copies of the ASP should segregate each section of the ASP into a standalone document as an editing document, then combine those sections in to a single viewable PDF format (if practical).
- Develop a template that predefines the document attributes, such as header and body text styles, and automatically inserts desired format elements, such as section breaks before each top-level header.
- To minimize disruptions during editing, anchor objects such as images and figures to the corresponding text.

Key Takeaways

1. Use a word processing software program that permits user-friendly editing capabilities.
2. Store each section of the ASP as a standalone file under a single file folder to allow for easier editing and formatting during the amendment process.

5.2 Document Storage Considerations

TSA has specific requirements for the handling and protection of SSI. Airports use two types of document formats for ASP storage and operational use: hard copy, and electronic files that are accessed with passwords or digital/electronic type storage with layered security protections. All airports use an electronic copy (working copy) of the ASP that is used for updates and amendments, these versions are also SSI and must be protected appropriately.

TSA has established the following requirements and best practices for the protection of SSI documents:

- Lock up all hard copies
- Protect electronic copies with a password or encryption

- Mark SSI documents with the required cover page, header, and footer

The largest component of interviewed airports used a combination of hard copy and electronically formatted approved ASP copies. A much lower percentage of airports had moved to digital format only. The results of the airport interviews for this research are detailed below:

- 18.2% of airports utilized electronic copies only
- 45.5% used both electronic and hard copies
- 36.3% were operating with hard copies only

The use of an electronically stored ASP greatly reduces the possibility that outdated copies of the ASP are being accessed for operational functions. It also simplifies the update and amendment process. Additionally, the use of an electronic-only ASP also allows for the immediate revocation of individual access privileges.

Key Takeaways

1. Almost half of all airports use both hard copy and electronic versions for their approved ASPs.
2. The industry is moving toward electronic-only ASPs.

SECTION 6: STAKEHOLDER COMMUNICATION STRATEGIES

Paramount to the task of managing an effective ASP from both administrative and operational perspectives is the airport's ability to promote, develop, and maintain a strong working relationship with TSA. The key to growing this relationship is centered on maintaining a flow of two-way communications that are open, timely, and accurate. The sections below provide guidance that can help assist ASCs in achieving this critical goal.

6.1 Effective Communication with the TSA

ASCs and TSA officials agree that maintaining a positive working relationship and ensuring the regular flow of effective communications between the two parties is a critical aspect to fulfilling the requirements of an ASP. Key components and tools related to accomplishing this communication goal include:

- The ability to agree on amendment language and intent is a necessity during the initial phases of the amendment drafting process.
- Maintaining ongoing contact with TSA through phone calls and meetings ensures that updates and changes affecting the airport are communicated in a timely fashion and are agreed upon in advance.
- Regularly scheduled meetings can also provide opportunities to discuss solutions to potential issues, thus helping to avoid last minute requests that sometimes cause delays in the approval process.

A variety of methods can be utilized to communicate effectively between airport security partners. The frequency, type, and level of formality used to transfer key information will vary based on the security category of the airport, but all airport categories share the duty of ensuring that relevant changes in security measures, protocols, and conditions at the airport need to be communicated in a timely manner to the TSA.

Methods that ASCs can use to disseminate key information to airport stakeholders and TSA will vary depending on some of the variables previously mentioned, but generally include the following:

- Verbal (face to face or telephone)
- In-person meetings (weekly, quarterly, or monthly)
- Badge holder required training
- E-mails (Security Bulletins, or informal correspondence)
- Community portals (access restricted)
- Newsletters for non-SSI information

The appropriate form of communication will vary based on the size of the airport and the timeliness of the information that is being provided. Table 6-1 lists examples of frequently used communication and coordination methods based on airport security category.

Table 6-1. Frequently Used Communication Methods Based on Airport Security Categories

Airport Category	Weekly Meetings	Monthly Meetings	Quarterly Meetings	Badge Training	Access Restricted Portals	Password-Protected Emails/ Bulletins	In Person – Verbal
X	X	X		X	X	X	
I	X	X		X	X	X	
II		X	X	X		X	
III			X	X		X	X
IV			X			X	X

It is strongly recommended that airports and their TSA partners have regularly scheduled one-on-one meetings to support focused and free discussion of upcoming issues.

One Cat X airport mentioned that they typically conduct weekly meetings with the TSA, often with no specific agenda. They stated that this meeting has proven to be very productive and has greatly improved the communication channels between the two entities.

As security information is transferred between TSA and the ASC, officials have occasionally noted perceived differences in the messages that TSA headquarters is disseminating versus the guidance from the local TSA field office. This is usually related to the intent of the information and the required implementation of new security directives or amendments. Airport ASCs are obligated to follow the directions of local TSA officials, but miscommunication and grey areas between TSA headquarters and their field offices can lead to a lack of clarity and disagreements on the associated implementation process at the airport level. Also, ASCs routinely use their network of ASCs and industry associations to monitor and assess new or upcoming security guidance and use this information to help determine the intent of new TSA directives.

Although these types of issues must be addressed on a case-by-case basis, it was noted that airports that regularly interact and communicate with their local TSA partners often identify potential issues far in advance and are able to resolve them in a proactive versus a reactive manner.

Key Takeaways

1. Establishing a strong working relationship between airports and the TSA is a critical component in ASP management.
2. Regularly scheduled meetings are an effective communication tool that can be used for all airports of all sizes.
3. Effective communication often results in proactive versus reactive response to potential issues.

5.2 Airport Internal Communications

The regular dissemination of appropriate security-related information to all levels of airport's security team is a key component to the overall effectiveness of the ASP. There should be internal communications between the airport security division and other key airport areas such as Operations, Maintenance, Legal, etc., so that respective areas of the ASP are understood.

Effective dissemination of ASP information, updates, and amendments can be enhanced by the following:

- Establishing strong working internal relationships between Primary ASCs, Alternate ASCs, and other key security staff
- Proactive communications and coordination with security staff will ensure that the information that needs to be delivered is received, understood, and handled appropriately in a consistent manner throughout the organization, and in accordance with the intent of the ASP or airport directives

Guidance from TSA will dictate who must receive ASP changes and other security-related information, and senior ASCs must ensure that this information is disseminated accordingly to all appropriate security staff using the methods described in this section.

Key Takeaways

1. ASCs and airport staff share the responsibility to help prevent terrorist activity
2. The dissemination of accurate, appropriate, and timely information to airport security staff is essential

REFERENCES

Aircraft Owners and Pilots Association. (2018, October 10). TSA Airport Access Security Requirements [Text]. https://www.aopa.org/advocacy/airports-and-airspace/security-and-borders/tsa-airport-access-security-requirements

Airport Security Program Sample Clauses. (n.d.). Law Insider. Retrieved September 5, 2023, from https://www.lawinsider.com/clause/airport-security-program

Ashford, N., Stanton, H. P. M., & Moore, C. A. (2013). Airport operations (Third edition). McGraw-Hill.

Benny, D. J. (2013). General aviation security: Aircraft, hangars, fixed-base operations, flight schools, and airports. CRC Press.

Critical Infrastructure Information Act (CIIA) of 2002, codified at 6 USC §§ 131–134.

Department for Transport. (2021). Framework for an Aviation Security Management System (SeMS). Civil Aviation Authority.

DHS. (2017). Handbook for Safeguarding Sensitive PII. DHS.

DHS. (2018). Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide Comprehensive Preparedness Guide (CPG) 201. Department of Homeland Security.

Dragos Blog. (2023, March 30). Preparing for TSA Cybersecurity Directive for Airports & Aircraft Operators | Dragos. https://www.dragos.com/blog/emergency-tsa-cybersecurity-directive-for-airports-aircraft-operators-how-to-prepare/

FAA. (2009). FAA Advisory Circular 150/5200-31C Airport Emergency Plan. FAA.

Faith Group, LLC. (2017). PARAS 0010: Guidance for protecting access to vital systems impacting airport security. National Safe Skies Alliance: Program for Applied Research in Aviation Security.

Faith Group, LLC. (2019). PARAS 0011: Guidance for airport security master planning. National Safe Skies Alliance: Program for Applied Research in Aviation Security.

FEMA. (2017). National Incident Management System. Federal Emergency Management Agency.

FEMA. (2021). Developing and Maintaining Emergency Operations Plans Comprehensive Preparedness Guide (CPG) 101. Federal Emergency Management Agency.

GAO. (2022). TSA should clarify compliance program guidance and address user concerns with its data systems (Report to Congress GAO-22-105063).

Ghobrial, A., & Fleming, K. (1994). A model for developing an airport security plan. Journal of Aviation/Aerospace Education and Research, 4(2).

Griffith, D., Bender, G., Ayodhiramanujan, K., Sayadi, N., Smith, J., Dodson, A., White, C., Sawyer, J., Quinn, J., & Williams, K. (2014). Airport Cooperative Research Program Report 112 Airport Terminal Response Planning. Transportation Research Board.

Home Office, Department of Transport. (2010). Airport Security Planning Quick Guide. Crown.

ICAO. (2022). ICAO Annex 17 to the Convention on International Civil Aviation, Aviation Security: Safeguarding International Civil Aviation against Acts of Unlawful Interference. International Civil Aviation Organization.

Johnstone, W. (2015). Protecting transportation: Implementing security policies and programs. Butterworth-Heinemann.

Madrid, R. (2022). Airport Cooperative Research Program Report Command-Level Decision Making for Transportation Emergency Managers Report 04-04. Transportation Research Board.

McGee, S., McCarthy, P., Evans Consulting, & Dynamis Inc. (2021). PARAS 0027 Guidance for Root Cause Analysis in Aviation Security. National Safe Skies Alliance: Program for Applied Research in Aviation Security.

Poisgrove, N., Gabrielson, N., & O'Krongley, T. (2021). PARAS 0037: Planning and operational security guidance for construction projects at airports. National Safe Skies Alliance: Program for Applied Research in Aviation Security.

Port Authority of New York and New Jersey. (2014). New York State Department of Transportation Aviation Bureau: Airport Security Plan. Port Authority of New York and New Jersey.

Port Authority of New York and New Jersey. (2019). Airport Security Guidelines Manual. Port Authority of New York and New Jersey.

Prather, C. D. (2015). Airport management. ASA, Aviation Supplies & Academics.

Price, J. (2022). Airport certified employee-security (Sixth). American Association of Airport Executives.

Price, J., & Forrest, J. (2016). Practical airport operations, safety, and emergency management: Protocols for today and the future. Butterworth-Heinemann.

Price, J., & Forrest, J. (2016). Practical aviation security: Predicting and preventing future threats. (Third). Butterworth-Heinemann.

Radio Technical Commission for Aeronautics. (2022). Standards for Airport Security Access Control Systems. RTCA.

Rieder, R. (2021). PARAS 0028: Recommended security guidelines for airport planning, design, and construction. National Safe Skies Alliance: Program for Applied Research in Aviation Security.

Rieder, R., Peel, S., & Swinstead, L. (2018). PARAS 0009: Guidance for security management systems (SeMs). National Safe Skies Alliance: Program for Applied Research in Aviation Security.

Romig, T. (2015). The hijacking of Flight ET 702: The challenges of managing a major security threat, media attention and continuing daily airport operations. Journal of Airport Management, 9(4).

Salus Solutions. (2021). PARAS 0026: Insider threat mitigation at airports. National Safe Skies Alliance: Program for Applied Research in Aviation Security.

San Jose Airport. (2023). Instructions for completing a security plan. San Jose Airport.

Schultz, M., Luo, M., Lubig, D., Mujica-Mota, M., & Scala, P. (2021). Covid-19 related challenges for new normality in airport terminal operations. Institute of Electrical and Electronics Engineers. Proceedings of the 2021 Winter Simulation Conference.

Security of air transport infrastructures of Europe. (2019). D7.3 – Best practices for updating airport security standard and policies. European Union's Horizon 2020 research and innovation programme.

SSI Policies and Procedures Handbook. (2015). TSA.

Stallings, M. & Faust, Whitney. (2009). Drafting, revising, and updating local emergency operations plans: The National Response Framework and the Emergency Support Function Annex model. Journal of Emergency Management, 7(2).

Stamburgh, H., Sensenig, D., Copping, Teresa, Argabright, M., Ockershausen, J., & Spencer, Lisa. (2009). Airport Cooperative Research Program Report 12 An Airport Guide for Regional Emergency Planning for CBRNE events. Transportation Research Board.

Stewart, M., & Mueller, J. (2018). Are we safe enough? Elsevier.

Thompson, S. (2016). Positioning airports for safety management system success. Journal for Airport Management, 16(4).

Title 49 Code of Federal Regulations Part 1520 (Protection of Sensitive Security Information), (2001).

Title 49 Code of Federal Regulations Part 1540 (Civil Aviation Security: General Rules), (2001).

Title 49 Code of Federal Regulations Part 1542 (Airport Security), (2001).

Title 49 Code of Federal Regulations Part 1544 (Aircraft Operator Security: Air Carriers and Commercial Operators), (2002).

Title 49 Code of Federal Regulations Part 1546 (Foreign Air Carrier Security), (2002).

Transportation Security Administration. Sensitive Security Information: SSI Quick Reference Guide for DHS Employees and Contractors.

Transports Canada. (2015). Industry Guidance: Airport Security Programs. Transport Canada.

TSA issues new cybersecurity requirements for airport and aircraft operators | Transportation Security Administration. (n.d.). Retrieved September 6, 2023, from https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

TSA. (2022). Sensitive Security Information Quick Reference Guide. TSA.

Young, S. B., & Wells, A. (2019). Airport planning and management (Seventh edition). McGraw-Hill Education.

Zoufal, D., Bender, G., Wendt, D., Entrekin, A., Gafford, J., & Cussan, S. (2021). PARAS 0025: Security regulatory compliance at tenant facilities. National Safe Skies Alliance: Program for Applied Research in Aviation Security.

Zoufal, D., Cussan, S., Freadman, M., Wendt, D., Gafford, J., & Pantle, M. A. (2023). PARAS 0008: Findings and Practices in Sharing Sensitive Information. National Safe Skies Alliance: Program for Applied Research in Aviation Security.

Zoufal, D., Cussan, S., Freadman, M., Wendt, D., Gafford, J., & Pantle, M. A. (2023). PARAS 0044: Strategies for Aviation Security Stakeholder Information Sharing (0044). National Safe Skies Alliance: Program for Applied Research in Aviation Security.

APPENDIX A: REFERENCE AND GUIDANCE DOCUMENTS FOR ASCS

Prior to engaging in the development of an Airport Security Program, ASCs should become familiar with, at a minimum, the following key documents:

- **ICAO. (2022). ICAO Annex 17 to the Convention on International Civil Aviation, Aviation Security: Safeguarding International Civil Aviation against Acts of Unlawful Interference.** ICAO Annex 17 serves as the cornerstone document upon which all airport security programs worldwide are founded. It is available through ICAO's website.
- While the Security Threat Assessment (STA) procedure for airport operators is primarily detailed in Security Directives, the overarching process for aircraft operators and other parties discussed in Part 1540 closely mirrors the airport STA process.
- **Radio Technical Commission for Aeronautics. (2022). Standards for Airport Security Access Control Systems. RTCA.** This document provides technical guidance on the implementation of numerous airport security related systems including identity management, physical access control systems, perimeter intrusion detection, video surveillance systems and communications infrastructure. It is available through the RTCA.
- **Rieder, R. (2021). PARAS 0028: Recommended security guidelines for airport planning, design and construction. National Safe Skies Alliance: Program for Applied Research in Aviation Security.** This is a valuable document that assists ASCs in constructing security areas, physical protection in both the public and security related areas, and other important topics. Although it does not directly address the development of an ASP, it does provide many of the elements required to be included in an ASP along with guidance on their implementation, such as physical access control systems, perimeter defense, and public area protection.
- **Title 49 CFR Part 1520 (Protection of Sensitive Security Information), (2001).** This regulatory document addresses the handling and dissemination of materials, marked Sensitive Security Information (SSI). ASPs are required to be marked as SSI.
- **Title 49 CFR Part 1540 (Civil Aviation Security: General Rules), (2001).** This regulatory document addresses several general rules of transportation, security, including topics, such as fraud, interference with security personnel, carriage of weapons on board an aircraft, and to an extent, Security Threat Assessments (STA). Part 1540 also includes the definitions of many terms used in aviation security.
- **Title 49 CFR Part 1542 (Airport Security), (2001).**
- **Transportation Security Administration.** ***Sensitive Security Information: SSI Quick Reference Guide for DHS Employees and Contractors*****.** This regulatory document most directly addresses the required content of an ASP.
- **Stephen Lehocky, Gloria Bender, & Jessica Gafford (2017).** ***PARAS 0008: Findings and Practices in Sharing Sensitive Information*****.** National Safe Skies Alliance: Program for Applied Research in Aviation Security. This document provides critical guidance on the sharing of SSI.

Relevant Security Directives (SD), Information Circulars (IC) and any airport, TSA local, or TSA National Amendments (NA). The following list is a starting point and is subject to change:

National Amendments

- TSA-NA-01-01 Airport Categorization
- TSA-NA-03-02 Airport Security Coordinator Training Curriculum
- TSA-NA-09-02 Security Tamper Evident Bags (STEBS)

- TSA-NA-11-01 Patrols
- TSA-NA-12-04 Response to SIDA Door Alarms
- TSA-NA-14-01 Incidents and Suspicious Activity Reporting
- TSA-NA-16-01 Inspection of Merchandise and Consumables Intended for the Sterile Area
- TSA-NA-16-02 Standardizing Knives In The Sterile Area
- TSA-NA-17-01 Security Measures - National Terrorism Advisory System (NTAS)
- TSA-NA-18-01 Airport Access and Vetting
- TSA-NA-18-03 Authorized Signatory
- TSA-NA-19-02 Airport Identification Media Audits
- TSA-NA-21-01 Centralized Revocation Database for Individuals with Revoked Identification Media
- TSA-NA-21-02 Ramp Movement
- TSA-NA-21-03 Criminal History Records Checks (CHRC) and the Federal Bureau of Investigation (FBI) Rap Back Program
- TSA-NA-21-05 Cybersecurity Incident Reporting
- TSA-NA-22-01 Cybersecurity Self-Assessments and Incident Response Plans
- TSA-NA-23-01 Public Advisories
- TSA-NA-23-02 Aviation Worker Screening
- TSA-NA-97-01 Airport Security

Security Directives

- SD 1542-04-08 STA and Reports
- SD 1542-04-10 Airport Tenant Access to the Sterile Area
- SD 1542-18-01 Threats to Airports

Emergency Amendment

- Joint EA 23-01 Cybersecurity – Performance-Based Measures

Operations Directive

- Operations Directive (OD)-400-50-5-5 Registered Traveler Programs

Order

- Cybersecurity Requirements for United States Airport Fueling Operations

It should be noted that the ASC must also have access to the Homeland Security Information Network (HSIN). The HSIN is accessed online and serves as a method of communicating information between airport and aircraft operators, and the TSA. ASCs can apply for access to the HSIN and certain security programs within the HSIN through their Federal Security Director.

ASCs may also benefit from reviewing existing ASPs from similarly sized airports. Note: an ASC may be asked to sign a non-disclosure agreement for another airport to share their ASP, and the other airports may also have to seek permission from TSA to share the ASP.

TSA has previously published guidance on complying with the CFRs, but those documents have since been rescinded. ASCs must rely on TSA personnel to know the regulatory requirements beyond those in

the CFRs. Therefore, ASCs must work closely with TSA to ensure local and national TSA requirements are being met. Additional guiding documents can be found in the Literature Review in Appendix D.

APPENDIX B: GLOSSARY

Where possible throughout this document, the specific regulatory definitions for the following terms are used. In other cases, the definitions have been created for the purposes of this document and are flexible in terms of industry standards. Further definitions can be found in CFR § 1540, SDs, NAs and other related documents.

ID Media: a form of identification that includes an individual's face, name, and a unique identification number, in addition to an encoded portion that acts as an access code to open doors, gates, etc. Commonly referred to as the airport identification badge. It is important to note that not all airport-approved identification also provides access.

Airport Tenant Security Program: the agreement between the airport operator and an airport tenant that specifies the measures by which the tenant will perform security functions, and approved by TSA, under Part 1542.113.

Authorized Signatory: the primary point of contact between the Airport Security Credentialing Office and companies for all airport security ID media / badging needs.

Changed Condition: a condition on the airport that is inconsistent with what is described in the ASP and may require notification to the TSA.

Designated Aviation Channeler: a private company that acts as a connection between the airport operator (and aircraft operator and others requiring such services such as flight schools), and the TSA and FBI, in conducting credentialing checks.

Exclusive Area Agreement: an agreement between the airport operator and an aircraft operator or a foreign air carrier that has a security program under Part 1544 or 1546 of this chapter that permits such an aircraft operator or foreign air carrier to assume responsibility for specified security measures in accordance with Part 1542.111.

Fixed-Base Operator: a tenant authorized by an airport to operate on its premises, offering a range of aeronautical services encompassing fueling, hangaring, tie-down and parking facilities, aircraft rental, aircraft maintenance, flight instruction, and other related services.

Full All-Cargo Security Program: an aircraft operator security program required for operators of aircraft carrying only, and requiring the screening of, all cargo on board.

Full Security Program: an aircraft operator security program that requires the screening of all passengers, baggage, and cargo.

Ground Security Coordinator: an individual that oversees compliance with the appropriate aircraft operator security requirements while the aircraft is on the ground (as opposed to when it is 'in-flight,' meaning all outer doors have been closed).

Known Crewmember: a TSA trusted crewmember program that allows certain approved aircraft operator personnel to use alternative forms of screening other than the passenger checkpoint.

Movement Areas: the runways, taxiways, and other areas of an airport that are used for taxiing, takeoff, and landing of aircraft, exclusive of loading ramps and aircraft parking areas.

Secured Area: a portion of an airport, specified in the airport security program, in which certain security measures specified in Part 1542 of this chapter are carried out. This area is where aircraft

operators and foreign air carriers that have a security program under Part 1544 or 1546 of this chapter enplane and deplane passengers and sort and load baggage and any adjacent areas that are not separated by adequate security measures.

Security Identification Display Area (SIDA): a portion of an airport, specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport.

Sterile Area: a portion of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator under Part 1544 of this chapter or a foreign air carrier under Part 1546 of this chapter, through the screening of persons and property.

Stop List: a list of ID media that has been invalidated, but the physical ID media has not been returned to the credentialing office.

Trusted Agents: are responsible for safeguarding sensitive and confidential information, assessing door access requests, facilitating access provision, and confirming the legitimacy and appropriateness of government-issued identification documents before issuing badges.

Unescorted Access Authority: the authority granted by an airport operator, an aircraft operator, foreign air carrier, or airport tenant under Part 1542, 1544, or 1546 of this chapter, to individuals to gain entry to, and be present without an escort in, Secured Areas and SIDAs of airports.

APPENDIX C: AIRPORT & TSA INTERVIEW QUESTIONS

Airports were asked the following series of ten questions by the Research Team. Many of the questions sparked additional discussion.

1. What Security Category Airport are you responsible for?
2. Do you operate/regulate a full, supporting, or partial program?
3. What are the top 5 challenges related to maintaining/regulating Airport Security Programs (ASPs) and how do you address them?
4. In addition to the issuance of SDs and NAs, what are other reasons that cause you to update or amendment your ASP?
5. What is your standard procedure used to initiate and finalize ASP updates? What is the review and approval process?
6. Do you use hard copy or electronic formats for your ASP? Please explain why you use the format that you use and any benefits to that format.
7. Do you use checklists or flow charts to assist you in implementing plans in an ASP? Please explain.
8. Describe the Primary versus Alternate ASC duties and responsibilities? What is the relationship between the two? How many alternates do you have?
9. How do you communicate changes in the ASP with stakeholders?
10. How do you protect SSI information contained in the ASP when you are amending and/or implementing new changes?

TSA representatives were asked the following ten questions by the Research Team. Many of the questions sparked additional discussion.

1. How many 1542 airports are you responsible for?
2. What are the primary differences in deciding on if they need a full, supporting, or partial program and what are the differences?
3. What are the top 5 challenges related to maintaining/regulating ASPs and how do you address them with your airports?
4. In addition to the issuance of SDs and NAs, what are other reasons that cause you to require updates or amendments for ASPs? (i.e., developing a new program, updating an existing program, or transitioning between programs… discuss maintenance of an existing program.)
5. What is your standard procedure used to initiate and finalize ASP updates? What is the ideal review and approval process, how can we improve the current process, what should be avoided?
6. Do you prefer the use of hard copy or electronic formats for an ASP? Please explain why and the format that you prefer and the benefits to that format.
7. If an airport operator is significantly amending or creating a new ASP, what guidance is available for them to reference? How do you support airports in the process? Do you have checklists or flow charts to assist you in creating a new ASP? Please explain.

8. Describe the Primary versus Alternate ASC duties and responsibilities? What do you see as the relationship between the two? How many alternates do you recommend an airport have?
9. How do you recommend that an airport communicate changes in the ASP with stakeholders?
10. How do you prefer that SSI is protected when an airport is amending and/or implementing new changes

APPENDIX D: LITERATURE REVIEW FINDINGS

In this case, the literature review provided limited results. While there is not as much written about the subject of drafting ASPs as much of the guidance information is SSI, some public guidance was discovered through existing textbooks, security certification programs and several existing PARAS reports. Due to the limited public information, we expanded our search to include other similar security and emergency plans, such as FAA Advisory Circulars, FEMA homeland security guidance and in some cases, international guidance.

The ASP explains how each individual airport will comply with the requirements of Title 49 CFR § 1542 – Airport Security (Part 1542). The ASP is drafted by the ASC and must be approved by the TSA's Federal Security Director before the airport can be approved for commercial flight operations. ASPs are only required at commercial service airports enplaning more than 2500 annual passengers. ASPs are not required for General Aviation airports (Price, 2022).

Once approved by TSA, an ASP is quite literally the "regulations" for that airport. No distinction is made between whether a requirement is in Part 1542 or within an ASP. Violating an element of the ASP is seen as the equivalent of violating an element of Part 1542 (Price & Forrest, 2016). Much of the information for constructing an airport security program was found in a couple of key documents: the textbook Practical aviation security: Predicting and preventing future threats (Price & Forrest, 2016), and the American Association of Airport Executives Airport Certified Employee-Security program (Price, 2022). Based on a review of the Airports Council International Programs and Services website, it appears that similar information on the construction of ASPs may also be discovered, but we did not obtain the training materials for these courses. Several other textbooks were referenced but provided only cursory information on the development of an ASP.

The Port Authority of New York to New Jersey provides publicly available documents on the contents of an ASP (Port Authority of New York and New Jersey, 2019). Through PARAS, National Safe Skies Alliance also provides several different documents that can assist ASCs in the development and upkeep of an ASP. By far the most useful document related to this project is PARAS 0028 *Recommended Security Guidelines for Airport Planning, Design and Construction* (Rieder, 2021). Although it does not directly address the construction of an ASP, it does provide many of the elements required to be included in an ASP along with guidance on their implementation, such as physical access control systems, perimeter defense, and security areas.

Another key document to support development of an ASP is the Radio Technical Commission for Aeronautics (RTCA) Standards for Airport Access Control Systems (RTCA, 2022). The RTCA document provides critical information on developing the airport's credentialing, physical access control system, video surveillance, security operations center, and security communications infrastructure.

Numerous other documents provided guidance in developing a component of an ASP and/or management of similar programs, such as emergency operation plans, that can be translated and incorporated into the development of an ASP.

The foundational document for developing and updating an ASP is Part 1542, which includes the required elements in an ASP and can be used as a "table of contents" of what must be included in the ASP. However, very little is provided in terms of how to comply with the regulations. Part 1542 explains "what" regulations an airport must comply with, while the ASP itself explains "how" a particular airport complies with Part 1542. Therefore, the ASC must determine how to best explain how their airport will comply with Part 1542.

Additionally, the Research Team only completed a cursory review of International Civil Aviation Organization (ICAO) Doc 8973-Restricted Aviation Security Manual, Thirteenth Edition 2022. Although not technically considered SSI, the document does require permission of the State (i.e., country security representative, such as TSA or DHS) to be viewed. The cursory review revealed that this document contains little direct information on developing ASPs at the local level. Most of the ASP guidance from ICAO relates to a nation-state developing a national airport security program. There is only one paragraph in ICAO Annex 17 Aviation Security that requires a nation-state to have individual security programs for each airport serving commercial operations, but the document provides no guidance on the content or management of such a program.

We have separated the research into four categories: ASP-Specific Guidance, Related Airport Security Guidance, Related Aviation Industry Guidance (non-security specific), and Federal Guidance.

AIRPORT SECURITY PROGRAM–SPECIFIC GUIDANCE

The airport security program specific guidance yielded a wide range of results, with some providing general information that should be included in an ASP, while others were very precise, providing not only specifics that must be included in an ASP, but also recommendations on how to implement the systems, methods, and procedures to comply with Part 1542.

Airport Security Program Sample Clauses. (n.d.). Law Insider. Retrieved September 5, 2023, from https://www.lawinsider.com/clause/airport-security-program
Addresses the legal foundation for certain airport identification badge holders.

Ghobrial, A., & Fleming, K. (1994). A model for developing an airport security plan. Journal of Aviation/Aerospace Education and Research, 4(2).
Provides a general overview of items to be included in an airport security plan (pre 9/11), but does not provide specifics in terms of how to comply with Part 1542 (nor Federal Aviation Regulation Part 107, which was the pre-9/11 security regulation).

Home Office, Department of Transport. (2010). Airport Security Planning Quick Guide. Crown.
This document, published by the United Kingdom, provides some guidance on identifying risks in the aviation environment. This is material to an ASC as risks must constantly be evaluated and mitigation and preparedness measures must be incorporated.

Johnstone, W. (2015). Protecting transportation: Implementing security policies and programs. Butterworth-Heinemann.
Provides limited guidance on drafting an ASP, but cites other works that are more comprehensive.

Port Authority of New York and New Jersey. (2014). New York State Department of Transportation Aviation Bureau: Airport Security Plan. Port Authority of New York and New Jersey.
Provides a very cursory overview of some topics to be included in an airport security plan. It should also be noted that the proper term is Airport Security "Program," not "plan."

Port Authority of New York and New Jersey. (2019). Airport Security Guidelines Manual. Port Authority of New York and New Jersey.
This document provides the closest model to an actual ASP as could be found in the public domain. It provides most of the information that must be included in an ASP and examples of regulatory compliance.

Price, J. (2022). Airport certified employee-security (Sixth). American Association of Airport Executives.
The "ACE-Security" modules explain exactly how to write and update an ASP, including a table of contents and guidance on complying with federal regulations. Guidance is provided in all areas of the ASP, including regulatory enforcement, updates to the ASP through Security Directives and National Amendments, distribution of SSI, and suggestions for establishing a distribution chain for copies of the ASP.

Price, J., & Forrest, J. (2016). Practical aviation security: Predicting and preventing future threats. (Third). Butterworth-Heinemann.
Chapter five of this text provides information like the ACE-Security program, but expands in other chapters upon the overall aviation security domain by explaining how screening processes and other regulatory requirements, such as how to design and implement incident management plans and contingency plans.

San Jose Airport. (2023). Instructions for completing a security plan. San Jose Airport.
Provides overall guidance on establishing an access control system.

Security of air transport infrastructures of Europe. (2019). D7.3 – Best practices for updating airport security standard and policies. European Union's Horizon 2020 research and innovation programme (sic).
Provides a tremendous amount of information on establishing an airport cybersecurity program.

Title 49 Code of Federal Regulations Part 1542 (Airport Security), (2001).
Provides the regulatory requirements for ASPs.

Transports Canada. (2015). Industry Guidance: Airport Security Programs. Transport Canada.
Provides information related to dissemination of risk- and security-related information.

RELATED AIRPORT SECURITY GUIDANCE

Faith Group, LLC. (2019). PARAS 0011: Guidance for airport security master planning. National Safe Skies Alliance: Program for Applied Research in Aviation Security.
https://www.sskies.org/images/uploads/subpage/PARAS_0011.SecurityMasterPlanning.FinalReport.pdf
Provides overall guidance in developing a security master plan. The document discusses dissemination of security information but not in detail.

Faith Group, LLC. (2017). PARAS 0010: Guidance for protecting access to vital systems impacting airport security. National Safe Skies Alliance: Program for Applied Research in Aviation Security.
Discusses security access controls and protection of other vital systems related to protecting access to the airport.

Department for Transport. (2021). Framework for an Aviation Security Management System (SeMS). Civil Aviation Authority.
Focuses primarily on threat and risk assessments, with some information related to cybersecurity.

Dragos Blog. (2023, March 30). Preparing for TSA Cybersecurity Directive for Airports & Aircraft Operators | Dragos. https://www.dragos.com/blog/emergency-tsa-cybersecurity-directive-for-airports-aircraft-operators-how-to-prepare/
Provides duplicate information already provided by TSA.

GAO. (2022). TSA should clarify compliance program guidance and address user concerns with its data systems (Report to Congress GAO-22-105063).
This report discusses the TSA's lack of guidance on regulatory compliance of airport and aircraft operator security programs.

Benny, D. J. (2013). General aviation security: Aircraft, hangars, fixed-base operations, flight schools, and airports. CRC Press.
This book focuses more on security at general aviation airports, but it does provide certain best practices that could be included in a commercial service ASP.

Griffith, D., Bender, G., Ayodhiramanujan, K., Sayadi, N., Smith, J., Dodson, A., White, C., Sawyer, J., Quinn, J., & Williams, K. (2014). Airport Cooperative Research Program Report 112 Airport Terminal Response Planning. Transportation Research Board.
Provides good information on items to include within an ASP.

ICAO. (2022). ICAO Annex 17 to the Convention on International Civil Aviation, Aviation Security: Safeguarding International Civil Aviation against Acts of Unlawful Interference. International Civil Aviation Organization.
Provides the international standard for aviation security regulations, but is very non-specific in providing content for individual airport security programs.

Madrid, R. (2022). Airport Cooperative Research Program Report Command-Level Decision Making for Transportation Emergency Managers Report 04-04. Transportation Research Board.
Useful for developing the incident management section of an ASP.

McGee, S., McCarthy, P., Evans Consulting, & Dynamis Inc. (2021). PARAS 0027 Guidance for Root Cause Analysis in Aviation Security. National Safe Skies Alliance: Program for Applied Research in Aviation Security.
https://www.sskies.org/images/uploads/subpage/PARAS_0037.AirportConstructionSecurity_.FinalReport_.pdf
Useful for identifying compliance issues within ASPs.

Poisgrove, N., Gabrielson, N., & O'Krongley, T. (2021). PARAS 0037: Planning and operational security guidance for construction projects at airports. National Safe Skies Alliance: Program for Applied Research in Aviation Security.
https://www.sskies.org/images/uploads/subpage/PARAS_0037.AirportConstructionSecurity_.FinalReport_.pdf
Provides critical information in handling the security requirements during construction on airports. Construction is one of the most common reasons ASCs submit amendments to TSA.

Radio Technical Commission for Aeronautics. (2022). Standards for Airport Security Access Control Systems. RTCA.
The guide for developing an airport's credentialing, perimeter intrusion, physical access control system, biometrics, video surveillance, and communications infrastructure in the airport security domain. A vital resource in the development of an ASP as it explains how to implement key elements of the ASP.

Rieder, R. (2021). PARAS 0028: Recommended security guidelines for airport planning, design, and construction. National Safe Skies Alliance: Program for Applied Research in Aviation Security.
https://www.sskies.org/images/uploads/subpage/PARAS_0028.Recommended_Security_Guidelines_.FinalReport_.pdf

The most complete document on guidance for establishing security areas and access control systems within the ASP.

Rieder, R., Peel, S., & Swinstead, L. (2018). PARAS 0009: Guidance for security management systems (SeMs). National Safe Skies Alliance: Program for Applied Research in Aviation Security. **https://www.sskies.org/images/uploads/subpage/PARAS_0009SeMS_Guidance-Final.pdf**
Focuses on the development of a Security Management System, but provides limited guidance on establishing or updating an ASP.

Salus Solutions. (2021). PARAS 0026: Insider threat mitigation at airports. National Safe Skies Alliance: Program for Applied Research in Aviation Security. **https://www.sskies.org/images/uploads/subpage/PARAS_0026_InsiderThreatMitigation.FinalReport_.pdf**
Provides guidance on airport worker security, which directly relates to new TSA requirements to screen airport personnel.

Stewart, M., & Mueller, J. (2018). Are we safe enough? Elsevier.
Mostly an academic look at the aviation security system overall without specific guidance in developing and maintaining and ASP.

TSA issues new cybersecurity requirements for airport and aircraft operators | Transportation Security Administration. (n.d.). Retrieved September 6, 2023, from **https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft**
Provides information on new cybersecurity requirements for airport operators. Although TSA has not been specific as to how this information will be incorporated into airport security programs, this website based on a national amendment includes the basic cybersecurity requirements.

Zoufal, D., Cussan, S., Freadman, M., Wendt, D., Gafford, J., & Pantle, M. A. (2023). PARAS 0008: Findings and Practices in Sharing Sensitive Information. National Safe Skies Alliance: Program for Applied Research in Aviation Security. **https://www.sskies.org/images/uploads/subpage/PARAS_0008.SharingSensitiveInfo.FinalReport.pdf**
An excellent resource in managing SSI documents and will contribute greatly to identifying, storing, tracking, and destroying information related to drafting and updating the ASP.

Zoufal, D., Bender, G., Wendt, D., Entrekin, A., Gafford, J., & Cussan, S. (2021). PARAS 0025: Security regulatory compliance at tenant facilities. National Safe Skies Alliance: Program for Applied Research in Aviation Security. **https://www.sskies.org/images/uploads/subpage/PARAS_0025.SecurityComplianceTenantFacilities_.FinalReport_.pdf**
Discusses Exclusive Area Agreements and Airport Tenant Security Programs, both of which are typically included in an ASP.

RELATED AVIATION INDUSTRY GUIDANCE (NON-SECURITY SPECIFIC)

Aircraft Owners and Pilots Association. (2018, October 10). TSA Airport Access Security Requirements [Text]. **https://www.aopa.org/advocacy/airports-and-airspace/security-and-borders/tsa-airport-access-security-requirements**
Provides an overview of airport security related to general aviation operations on commercial service airports.

Ashford, N., Stanton, H. P. M., & Moore, C. A. (2013). Airport operations (Third edition). McGraw-Hill.
Provides general guidance on aviation security.

FAA. (2009). FAA Advisory Circular 150/5200-31C Airport Emergency Plan. FAA.
Provides guidance on developing the Airport Emergency Plan and maintenance of the plan, some of which may be utilized in developing a notification and maintenance system of an ASP.

Prather, C. D. (2015). Airport management. ASA, Aviation Supplies & Academics.
Provides a general overview of airport security requirements.

Price, J., & Forrest, J. (2016). Practical airport operations, safety, and emergency management: Protocols for today and the future. Butterworth-Heinemann.
Provides a general overview of airport security requirements. It provides information on the implementation of safety management systems including creating and updating an existing SMS and information stakeholders of current and evolving safety risks. This information may be transferable to the security domain.

Romig, T. (2015). The hijacking of Flight ET 702: The challenges of managing a major security threat, media attention and continuing daily airport operations. Journal of Airport Management, 9(4).
Discusses security threat and airport operations during an incident.

Schultz, M., Luo, M., Lubig, D., Mujica-Mota, M., & Scala, P. (2021). Covid-19 related challenges for new normality in airport terminal operations. Institute of Electrical and Electronics Engineers. Proceedings of the 2021 Winter Simulation Conference.
Although not directly related to security, this document did bring up issues to consider, that could relate to maintaining airport security requirements during a communicable disease outbreak.

Stamburgh, H., Sensenig, D., Copping, Teresa, Argabright, M., Ockershausen, J., & Spencer, Lisa. (2009). Airport Cooperative Research Program Report 12 An Airport Guide for Regional Emergency Planning for CBRNE events. Transportation Research Board.
Discusses the upgrading of existing emergency plans to better coordinate with other jurisdictions in the planning of CBRNE events. There may be some material that can crossover to the airport security domain in terms of working with federal, state, and local response agencies to airport incidents.

Thompson, S. (2016). Positioning airports for safety management system success. Journal for Airport Management, 16(4).
Although related to safety management systems, there are some elements that can crossover to the security domain, particularly in terms of keeping stakeholders updated on risk assessments and mitigation procedures.

Young, S. B., & Wells, A. (2019). Airport planning and management (Seventh edition). McGraw-Hill Education.
Provides a general overview of airport security requirements.

NON-AVIATION

Critical Infrastructure Information Act (CIIA) of 2002, codified at 6 USC §§ 131–134.
Attempts to facilitate better sharing of critical infrastructure information amongst government agencies to reduce vulnerabilities.

Stallings, M. & Faust, Whitney. (2009). Drafting, revising, and updating local emergency operations plans: The National Response Framework and the Emergency Support Function Annex model. Journal of Emergency Management, 7(2).
Provided overall guidance on developing emergency operations plan is which are compliant with federal guidelines and requirements.

FEDERAL GUIDANCE

DHS. (2018). Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide Comprehensive Preparedness Guide (CPG) 201. Department of Homeland Security.
Discusses the identification of threats using risk assessments, which can translate to the aviation security domain, and potentially be included in the incident management sections of an ASP.

DHS. (2017). Handbook for Safeguarding Sensitive PII. DHS.
Provides information to safeguard personally identifiable information, which is critical in the ASP credentialing requirements under Part 1542.

FEMA. (2021). Developing and Maintaining Emergency Operations Plans Comprehensive Preparedness Guide (CPG) 101. Federal Emergency Management Agency.
Provides guidance on developing federally compliant emergency operations plans.

FEMA. (2017). National Incident Management System. Federal Emergency Management Agency.
Discusses the requirements of federal, state, and local agencies to use the Incident Command System.

TSA. (2022). Sensitive Security Information Quick Reference Guide. TSA.
A one-page handout for personnel on handling SSI.

TSA. Sensitive Security Information: SSI Quick Reference Guide for DHS Employees and Contractors.
Provides a general overview for handling SSI data and materials.

SSI Policies and Procedures Handbook. (2015). TSA.
Provides a more detailed account of handling Sensitive Security Information; this is an expansion of the SSI Quick Reference Guide.

APPENDIX E: CHECKLISTS FOR CREATING & REVIEWING THE ASP

CHECKLIST FOR CREATING THE ASP

Tasks	Completed?
Review the regulations under CFR Part 1542.101, .103, .105, .107	
Meet with TSA regulatory (i.e., inspection) personnel for guidance on developing the ASP	
Identify the required security program (Complete, Supporting, or Partial)	
Draft a Table of Contents based on the required type of security program	
Consult with the Security Consortium and other significant airport users	
Clearly mark the ASP as SSI per CFR Part 1520	
Include a Submittal page	
Include a Record of Amendments page	
Define the purpose of the ASP	
Describe the airport's location and category	
Describe the membership of the Security Consortium	
Describe the responsibilities of the ASC	
Identify the Primary ASC and alternate ASCs and their point-of-contact information	
Describe ASC training requirements	
Review all relevant Security Directives, local and National TSA Amendments and Information Circulars	
Include the procedures for distribution, storage, disposal of security programs, information circulars, implementing instructions and other classified information	
Include Abbreviations and Definitions	
Describe the security areas, barriers and the access control systems, measures, and procedures to control access between security areas and the public areas; security areas should also include any Exclusive Area Agreements and Airport Tenant Security Programs	
Describe the credentialing process and the personnel identification systems	
Describe law enforcement support of the ASP	
Describe the Contingency Plans	
Describe the Incident Management Plans	
Describe the method for keeping the public advised of airports that do not have effective security measures as determined by the DOT	
Describe alternate security procedures in the event of natural disasters or other emergency or unusual conditions.	
Draft an airport enforcement program	
Create rules and regulations related to airport security	

CHECKLIST FOR REVIEWING THE ASP

#	Description of Content 1542.103	Reviewed Current (c) or Not Current (nc)	Regulatory Reference Page (s)	Resolved Date
1.	**ASC Information**			
2.	Blank			
3.	**Secured Areas**			
4.	**AOA Areas**			
5.	**SIDA Areas**			
6.	**Sterile Areas**			
7.	**Procedures for CHRC**			
8.	**Personnel ID systems**			
9.	**Escort Procedures**			
10.	**Challenge Procedures**			
11.	**Training Programs**			
12.	Law Enforcement Support			
13.	Record Maintenance			
14.	**Screening Procedures**			
15.	Contingency Plan			
16.	SSI Dissemination			
17.	**Posting Public Advisories**			
18.	Incident Management Procedures			
19.	Alternate Security Procedures			
20.	Exclusive Area Agreements			
21.	Airport Tenant Security Programs			
22.	**Review compliance with all current EAs, NAs, and ICs**			

***Bold sections should be completed during Partial Reviews**