PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0025 April 2021

Security Regulatory Compliance at Tenant Facilities

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Donald Zoufal
CrowZnest Consulting, Inc.
Chicago, IL

Gloria Bender
Douglas Wendt
Andy Entrekin
Jessica Gafford
TransSolutions, LLC
Fort Worth, TX

Sean Cusson
Del Ray Solutions LLC
Washington, D.C.

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 0025 PROJECT PANEL

Kim Dickie *Port Authority of New York and New Jersey*
Tracy Fuller *ACTS – Aviation Security, Inc.*
Kelly Hoggan *H4 Solutions*
Daniel Oster *Children's Wisconsin*
Mike Pilgrim *International Security Concepts*
Renè Rieder *Burns Engineering*
Jeremy Worrall *State of Alaska Department of Transportation*

AUTHOR ACKNOWLEDGEMENTS

The research conducted for this Guidebook was performed by CrowZnest Consulting with the assistance of TransSolutions, LLC and Sean Cusson.

Donald Zoufal of CrowZnest Consulting was the Principal Investigator for the project and primary author of the guidebook. Sean Cusson, Douglas Wendt, Andy Entrekin, and Jessica Gafford assisted with the research and data collection.

The Research Team would like to acknowledge the airports who took time out of their busy schedules to help make this Guidebook robust and useful to all sized airports. It is only through the support of airports that Safe Skies is able to continue to provide the aviation industry with valuable research on practical airport-related topics. Finally, the Research Team wants to thank the panel of volunteers who lent their expertise and time to ensuring the Guidebook would be useful and applicable.

CONTENTS

SUMMARY

Tenant security arrangements present challenges and opportunities for all airports, large and small. Airports of all operating sizes include tenant security responsibilities in a wide array of tenant agreements that do not have a standard form or template. These agreements vary depending on the type of facility and designated facility operator. The options for managing tenant security arrangements come from several sources, including federal regulations, lease agreements, or local regulations. Further, known vulnerabilities require unique language in tenant agreements.

To date, there has not been a comprehensive guidebook or compendium to assist airports in structuring tenant security arrangements. Most airports looking for tenant security agreement language reach out to other airport operators for examples. This approach is helpful, but a more comprehensive picture of alternatives will likely lead to more satisfactory arrangements for both airport operators and tenants.

This toolkit provides descriptions of tenant security practices used by a wide range of airport stakeholders, and can assist in airports' assessments of tenant security responsibilities at their facilities. Although the overall responsibility remains with the airport operator, both federal regulations and other management tools like lease provisions or local regulatory programs enable the airport to shift some of the onus of maintaining a secure environment to other entities operating on airport property.

This toolkit explores the range of operational security challenges that tenant security agreements must address, and examines the approaches that have successfully met those challenges. To assist airports in constructing their own agreements, this toolkit provides a collection of language from different agreements, lease structures, and local regulations addressing tenant security issues. The example language provides a starting point for airport operators' considerations.

Additionally, to give readers a place to start, an assessment worksheet is included to help airport decision makers identify whether a centralized, non-regulatory agreement or a decentralized, regulated approach is best suited to their situations.

PARAS ACRONYMS

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

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ACC	Airport Control Center
ACS	Access Control System
ASC	Airport Security Coordinator
ASM	Airport Security Manager
ASP	Airport Security Program
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
ATSP	Airport Tenant Security Program
CACS	Computerized Access Control System
CAT	Category
CBP	Customs and Border Protection
CD	Compact Disc
CHRC	Criminal History Records Check
DA	District Attorney
DOA	Department of Aviation
DOT	Department of Transportation
EAA	Exclusive Area Agreement
FBO	Fixed-Base Operator
ID	Identification
LEO	Law Enforcement Officer
SASO	Specialized Aviation Service Operation
STA	Security Threat Assessment

SECTION 1: INTRODUCTION

Airports are complex enterprises with numerous tenants operating on their properties. Responsibility for airport security rests with the airport operators, while tenants cooperate and support their airport's security framework. Understanding the variety of tenant functions at airports is an important first step in incorporating tenants into an airport's security plan.

The number and types of tenant operations conducted at airports vary widely. Those operations include:

- Air carriers
- Fixed-based operators (FBO) and aircraft fuel farms
- Cargo operation facilities
- Private aircraft charter companies, seaplane operators, and tour operators (bus, helicopter, etc.)
- Servicing operations, such as maintenance (aircraft and airfield) and catering
- Concessionaires (retail, food and beverage, duty free shops, etc.)
- United Service Organization (USO) locations
- Deicing companies
- Police and fire stations
- ARFF training facilities and universities
- Offsite goods screening companies
- Federal offices
- Military bases
- Aircraft hangars
- Mailing facilities
- Cruise ship operators
- Remote bag-drop operators
- Museums

The nature of a tenant's operations and knowledge of security operations are important factors for consideration in the development of security arrangements. Tenant-controlled facilities often form a portion of airport perimeters, which means that they are inherently integral to an airport's security posture, particularly in regulated areas, and also in non-regulated but restricted areas of airports. Managing security for the areas occupied by tenants and their operations is a critical part of overall airport security. However, the variety of operations and scales of these facilities makes standardized templates difficult to prepare.

The current regulatory environment does provide some specific tools for direct inclusion of tenants in security operations. Though not widely utilized, federal regulations specifically recognize Exclusive Area Agreements (EAA) under 49 CFR § 1542.111, and Airport Tenant Security Programs (ATSP) under 49 CFR § 1542.113. Additionally, 49 CFR §§ 1544.227 and 1544.231 require aircraft operators to establish security programs for their facilities. Airports may also manage certain security functions of tenant organizations through their Airport Security Programs (ASP), developed and implemented under 49 CFR § 1542.103. For example, through their ASPs, airports already manage unescorted access to the Secured Area, Sterile Area, SIDA, and AOA. This includes activity by tenant employees who are issued ID media. Many airports create other forms of tenant security agreements that are incorporated into their ASP. These agreements supplement and provide more detailed requirements than those ordinarily found in an ASP.

Other measures that can be implemented to address collective security responsibilities include contractual arrangements in the form of leases, memorandums of understanding, or airport use agreements.

The key to success in structuring security arrangements with a tenant organization is a mutual understanding of the division of security responsibilities, and a clear demarcation of those

responsibilities within the agreement. This will be more easily achieved if each party understands the other's viewpoints and priorities. Like any other aspects of airport operations, a collaborative environment in problem solving generally produces the most effective results.

1.1 Purpose

Airports of all sizes have a need for tenant security agreements, but there is no standard template available. Additionally, the agreements may vary widely depending on the type of facility and designated facility operator, and require unique language based on the facility type. Because no template is available, airports contact other airport operators to receive examples that they can modify to suit their unique circumstances.

This toolkit enables readers to examine practices across a wide range of airport stakeholders and identify the various ways security responsibilities can be shared at the airport. The goal of this toolkit is to help inform the decisions of airport operators when developing regulatory policies, contractual agreements, or other enforceable security arrangements concerning entities operating on airport property.

1.2 Scope

This toolkit was designed to assist airports of all sizes when developing airport-tenant security arrangements. It identifies the range of operational security challenges that need to be addressed in tenant security, and it examines the approaches that have been successfully undertaken to meet those challenges.

The toolkit is not intended to be a "one size fits all" template, as each agreement will have unique requirements based on facility type, operator, and operations. Rather, it includes a collection of language from differing agreements, lease structures, and local regulations addressing the issue of tenant security. This provides airports with an à la carte selection of language on a range of functional topics to consider when addressing their concerns regarding tenant security arrangements.

1.3 How to Use this Toolkit

This toolkit will serve as a primer for airports looking to establish or enhance their tenant security program. The table below outlines the topics discussed in the toolkit enabling readers who would like to find content most relevant to their specific areas of interest.

SECTION 2: Airport Approaches to Tenant Security Management		
2.1	Tenant-Centric Control Approach	Approaches to placing security responsibility on the tenant
2.2	Airport-Centric Control Approach	Approaches for airports to maintain security decisions
2.3	Identifying the Airport's Approach	Identifying the most appropriate approach for airport security
SECTION 3: Compliance Mechanisms		
3.1	Defined Federal Regulation	Discussions on federal security provisions, including EAAs and ATSPs

3.2	Ad Hoc Federal Regulation	Discussions on security provisions with federal oversight and compliance mechanisms, including ASP provisions, other tenant security programs, and badging regulations
3.3	Non-Federal Measures	Discussions on security provisions with state or local oversight and compliance measures, including leases, rules and regulations, and licensing/certification/permits
3.4	Credentialing	Discussions on training provided during the credentialing process, as well as utilizing Authorized Signatories for communicating security expectations to badge holders
SECTION 4: Critical Functions of the Agreement		
4.1	Access Control	Discussions and sample language on establishing access control protocols
4.2	ID Management	Discussions and sample language on issuing airport ID media
4.3	Challenge	Discussions and sample language on challenge procedures
4.4	Escort	Discussions and sample language on escort procedures
4.5	Training	Discussions and sample language on training stakeholders, including tenant employees and contractors working in tenant areas
4.6	Inspection	Discussions and sample language on inspection procedures of documents and physical inspections of tenant areas
4.7	Audit	Discussions and sample language on audit procedures of tenant agreements and documents
4.8	Security Personnel	Discussions and sample language on establishing security personnel requirements
4.9	Security Practices	Discussions and sample language on establishing security practices for security personnel, including training requirements
4.10	Changed Conditions	Discussions and sample language on changed condition notification and response requirements
4.11	Notice of Events or Incidents	Discussions and sample language on notice and reporting provisions
4.12	Sanctions	Discussions and sample language on monetary and non-monetary penalty provisions, including indemnity/hold harmless, liquidated damages, fines and penalties, suspension and revocation, and hearing/review and appeals processes
SECTION 5: Infrastructure and Equipment to Support Tenant Security Programs		
5.1	Access Control Infrastructure	Discussions and sample language on control of infrastructure to support access control, including lock and key, and automated access control systems (ACS)
5.2	Signage	Discussions and sample language on posting and maintaining signage at access points
5.3	Lighting	Discussions and sample language on lighting considerations around tenant areas

SECTION 5: Infrastructure and Equipment to Support Tenant Security Programs		
5.4	Fencing	Discussions and sample language on the installation and maintenance of perimeter fencing
5.5	Clear Zones	Discussions and sample language on clear zone requirements
5.6	CCTV	Discussions and sample language on CCTV controls and coverage, including the use and dissemination of the images generated by the system
SECTION 6: Agreement Preparation, Creation, and Review		
6.1	Drafting Agreements	Discussion on how to draft agreements with relevant security requirements; includes a checklist of common security requirements
6.2	Creating a Template	Discussion and suggestions for creating agreement templates
6.3	Maps and Floorplans	Discussion on creating and maintaining maps and floorplans of tenant spaces
6.4	Amending Agreements	Discussion on amending agreements and issuing temporary amendments for special events
6.5	Agreement Audits	Discussion on document management and annual reviews of security agreements
APPENDIX A: Assessment Worksheet to Identify Suitability for EAA/ATSP		
A worksheet designed to help airport decision makers identify the approach best suited for their security situation and needs		
APPENDIX B: Examples from Direct Federally Regulated Agreements		
Provides sample language and sample templates from EAAs and ATSPs		
APPENDIX C: Examples from Ad Hoc Federally Regulated Arrangements		
Provides sample language and sample templates from ASP provisions, other tenant security programs, and badging regulations		
APPENDIX D: Examples from Non-Federally Regulated Arrangements		
Provides sample language and sample templates from leases, rules and regulations, and licensing/certification/permits		

While there is no single or best way to manage airport tenant security requirements, this review of practices that have been successfully employed in airports large and small will help to better prepare an airport operator for addressing the needs of their airport.

SECTION 2: AIRPORT APPROACHES TO TENANT SECURITY MANAGEMENT

There are two different approaches to airport-tenant relationships regarding security and the performance of security functions, characterized as **tenant-centric control** and **airport-centric control**. These approaches should be seen as opposite ends of a continuum concerning the exercise of direct control over security operations. While the approaches can result in different allocations of functions between airports and tenants, most airports agree that the ultimate responsibility for airport security rests with the airports.

The approach an airport may select—with respect to the security of tenant facilities—is influenced by a variety of factors:

- Physical factors
  - Airport location and layout
  - Configuration
  - Infrastructure
- Operational factors
  - Airport passenger and cargo volumes
  - Scope of the tenant operation
- Legal factors
  - Governing body regulations
  - Local regulations
  - State regulations
  - Federal regulations
- Cultural factors
  - Relationships with airport tenants
  - Management philosophy
  - Nature of the security operation
- Risk factors
  - Airport's approach to risk
  - Tenant's approach to risk
  - Perception of risk
  - Measures for risk mitigation

The size of an airport alone does not necessarily affect the types of security arrangements chosen. As an example, some airports, large and small, reject the concept of using EAAs while other, similarly sized and situated airports embrace those types of agreements. In general, the airport's relationship with the TSA has a bigger impact on the selection of tenant arrangements. Some airports feel that enforcement for tenant non-compliance is more likely to be directed against the tenant and not the airport, at least in the first instance; these airports often choose informal arrangements in the form of lease agreements or other non-federally regulated agreements. Conversely, airports that feel that TSA enforcement would be directed against the airport often choose federally regulated agreements such as EAAs.

Tenants generally understand and are committed to providing proper security for their facilities, however, they differ greatly in their skills and experiences when working in a regulated high-threat environment like an airport. Some tenants such as airlines, cargo carriers, and aircraft servicing companies have large and sophisticated security operations and they have experience working in the

aviation industry's complex regulatory environment. Other tenants that are smaller entities or large entities that operate outside the airport environment, such as corporate hangars for private firms, tend to have less mature security operations with less experience in aviation regulatory compliance.

Security interest and culture also differ between organizations. While the airport and tenant security goals frequently align, there can be instances where the tenant gives higher priority to achieving other goals. Most tenants have the need to protect their facilities and the contents of those facilities, as well as safeguard the confidentiality of processes taking place within the facilities, even from the airport. These could include processing cargo, or aviation manufacturing and testing processes.

2.1 Tenant-Centric Control Approach

A tenant-centric control approach places security responsibility on tenants in areas of the airport where they operate and have a leasehold interest. The proportion of control over an area dictates the amount of security responsibility the tenant will take over for the area in question. For example, where an airline has a leasehold control and exclusively performs operations in an area such as a terminal, hangar, or cargo area, an airport might cede security authority over that area under an EAA. An airline or tenant that exercises more limited control over an area or exclusive control over a smaller area may have a different security agreement that prescribes control over more limited components of a security program. Airports may choose a tenant-centric control approach in circumstances where the tenant has more familiarity with the unique security and operational needs of the area, or where the tenant-centric strategy enables the airport to allocate resources to other needs.

Many tenants have expressed a strong preference for controlling security at their own facilities. The greater the proprietary function and the more complex the operation, the greater the preference for maintaining control. Most tenants focus less on the legal or regulatory structure of the arrangements and are more concerned with their ability to provide independent physical security of their facilities. However, even large and complex operations differed in their arrangements, as demonstrated by the implementation of EAAs at some airports and no agreements at others.

2.1.1 Factors Influencing Tenant-Centric Control Approach

A myriad of factors impacts whether a tenant-centric control approach fits best with an airport's security, business, and operational posture. The impacts of these factors vary from airport to airport and tenant to tenant.

While not directly correlated with airport sizes, in some instances the tenant-centric control approach is driven by the scale and complexity of the tenant operations relative to that of the airport. As an example, some smaller airports with large cargo hub operations have found that execution of an EAA relieves some pressure put on limited airport staff. Larger airports that have implemented EAAs appreciate the more direct accountability for tenant operations.

Airport culture and partnership strategy influence their needs for more formal security arrangements. Airports with greater confidence in the capabilities of tenant organizations may be more comfortable with arrangements, like EAAs, in which airport control and direct oversight responsibilities are reduced. Similarly, in cases where a greater focus on direct engagement of the tenant in security and formalized relationships with tenants exist, regulatory solutions like EAAs or ATSPs—rather than simple reliance on the provisions of ASPs—are often preferred.

2.1.2 Advantages and Disadvantages

Some of the advantages of a tenant-centric control approach include:

- Greater targeted engagement of tenants—airports using this approach state that tenants are more engaged in security.
- Security is better tailored to the tenant's needs—this advantage is more impactful when the tenant operation is complex of large in scale. Airports generally agree that the tenant has a better understanding of their unique security requirements.
- More effective utilization of tenant security experience—in some cases, particularly with respect to large cargo carriers, airports recognized that the level of tenant security experience and access to security resources was greater than that of the airport.
- Shift of operational and capital cost—moving security functions to the tenant allows the airport to shift direct security-related infrastructure and operational cost to the tenant organizations.
- Shift of liability—some airports see tenant agreements like EAAs and ATSPs as an opportunity to move liability for security failures, particularly TSA fines and penalties, to the tenant.

Some of the disadvantages of a tenant-centric control approach include:

- Loss of centralized control and flexibility—the shifting of security functions eliminates direct control over security operations. This may hinder the airport's ability to quickly adapt to changing threats and vulnerabilities.
- Concern about information flow and accurate understanding of airport security posture—airports are forced to rely on tenant actions and operations outside of the immediate control of the airport. These concerns can be mitigated by developing close relationships with tenants and impressing upon them the importance of timely notifications. Airports can also implement notification requirements in their agreements with tenants.

2.2 Airport-Centric Control Approach

Airport-centric control approaches seek to reserve most of the security decisions for the airports. Airports applying this approach directly supervise security operations to ensure that tenant efforts meet the airport's security goals.

2.2.1 Factors Influencing the Airport-Centric Control Approach

Airports often choose to exercise more direct control of security at their facilities. The security culture of the airport is frequently a driver in this decision. Rather than relying on other entities for enforcement, the airports taking this approach typically prefer to maintain responsibility for security to ensure the high security standards of the airport are met. They also expressed that, given the risk to reputation and brand, tight centralized control over security operations was critical.

2.2.2 Advantages and Disadvantages

Some of the advantages of using an airport-centric control approach include:

- Direct airport control over security—airports retain maximum flexibility in making changes to security strategies and arrangements to adapt to changing threats and vulnerabilities.
- Greater consistency in security arrangements—airports can ensure that security protocols are uniformly applied in all areas of the airport.

- Better situational awareness—airports have better access to information and direct control over the security posture in all areas of the airport, as well as faster notice of security vulnerabilities.
- Overcoming inconsistent security goals—airports have an enhanced ability to align tenant security goals with those of the airport.

Some of the disadvantages of using an airport-centric control approach include:

- Reduced tenant emphasis on security—with airports assuming principal responsibility for security, maintaining tenant focus on security becomes more challenging. Conducting regular security meetings with all tenant stakeholders is one way to emphasize tenant security responsibilities.
- Increased cost—airports' assumption of security responsibilities places greater financial responsibility on the airport for establishment and operation of infrastructure required to support security functions.
- Increased airport liability—airports' assumption of primary responsibility for security of tenant areas places greater liability on airports from both a regulatory and litigation standpoint.

2.3 Identifying the Airport's Approach

The approach airports take to centralize control over security may help them identify which of the methods outlined in the next sections are appropriate for implementing tenant security measures at their facilities. Appendix A provides an assessment worksheet designed to help airport decision makers identify whether an airport-centric, non-regulatory agreement or a tenant-centric, regulated approach is best suited for their situation. This worksheet can be completed before or after reading the remaining guidance.

SECTION 3: COMPLIANCE MECHANISMS

This section examines several compliance mechanisms available to assist airports in managing tenant security arrangements. Some of those measures involve federal regulation and others are creations of state or local arrangements of private leases. Federal regulations can come in two forms: defined regulatory governance under arrangements like EAAs or ATSPs or *ad hoc* federal regulation through provisions added to an ASP or the execution of other tenant agreements. Local regulations and agreements allow tenant arrangements to be managed without involving federal compliance measures.

3.1 Defined Federal Regulation

Federal regulations only define two specific tenant security arrangement types: EAAs and ATSPs. Both types of agreement, upon completion and approval, are required to be incorporated in airport's ASP. While moderate use has been made of EAAs, little use has been made of ATSPs.

For a significant period of time, many airport operators chose not to pursue formal regulatory structures like EAAs and ATSPs due to the perceived difficulty in securing TSA approval for them. This has resulted in many airports questioning the value of such formal regulatory arrangements. However, the research demonstrated that several airports of all sizes have used EAAs or other similar agreements and found they are excellent tools to manage security.

3.1.1 EAAs

EAAs, authorized under 49 CFR § 1542.111, permit otherwise regulated entities such as airlines, foreign air carriers, or air cargo airlines to assume security responsibilities in areas under their sole control. The agreements must meet all the Part 1542 requirements, must be included in the ASP, must be approved by TSA, and under the approved agreement, the regulated entity must also maintain a program under 49 CFR §§ 1544 and 1546. The EAA must include:

- Descriptions (maps and diagrams) that delineate the area of exclusive use and identify all access points
- A description of measures to provide security for Secured Areas,[1] AOAs,[2] or SIDAs[3] located within the EAA
- Procedures for notifying the airport of changed conditions[4]

Aircraft operators are required to report EAAs to the TSA and comply with EAA requirements.[5] EAAs are not considered a leasehold agreement, and the requirements of a leasehold agreement do not substitute for an EAA.

EAAs are predominantly utilized in connection with cargo operations. In some limited cases, EAAs have been used in connection with air carrier-exclusive terminal facilities. EAAs are employed in many airports regardless of security category designation, although they are most commonly employed at larger Category (CAT) X to CAT 2 airports. However, the structure of these agreements varies from airport to airport. Some airports establish detailed agreements for EAAs while other airports have more general agreements that are more narrowly focused on the requirements than the details of how they will

[1] 49 CFR § 1542.201
[2] 49 CFR § 1542.203
[3] 49 CFR § 1542.205
[4] 49 CFR § 1542.103 (a)
[5] 49 CFR § 1544.227

be met. In any case, all the requirements specified in Part 1542 must be met. Additional measures can, however, be specified in addition to the baseline requirements. Examples of both have been authorized by the TSA.

Many airports, especially smaller airports, claim that they cannot enact EAAs because their terminal space is shared among several air carriers. The TSA regulations note that the exclusive use of an area is required for an EAA, and the TSA will not approve an EAA in an area shared among multiple parties. However, in at least one airport TSA has approved an exception whereby an air carrier consortium operates under the EAA. The consortium consists of four air carriers that share the terminal. In this example, the EAA responsibility rotates annually among the air carriers. While this may not be an option for many airports, some may be able to work with their air carriers or other regulated entities in a shared space to create a similar agreement.

Airports that have established broadly drafted agreements for EAAs follow a format that includes provisions for the following:

1. Description of the EAA area
2. Access control procedures at all AOA, Secured Area, and SIDA access points
3. Challenge procedures
4. Escort procedures
5. Signage and notice requirements
6. Training requirements
7. Changed conditions procedures
8. Special circumstances

While EAAs do not have to mirror ASP security requirements, TSA will likely look for an equivalency in measures. This means that the differing security measures need to achieve the same security result. For example, using an automated ACS to secure a gate or portal is equivalent to using a lock and key system or the posting of security personnel.

In creating a general EAA, airports must be mindful that some degree of specificity is still required. Although blanket statements may serve to meet regulatory requirements, some details will need to be provided regarding how the specified security provisions will be executed and who will execute them.

The EAA must also contain provisions for immediate notification to the airport and alternative security measures to be executed in response to any changed condition.[6] For example, posting of security personnel to protect an area of fencing that has been destroyed until repairs can be made, or to staff an access gate where there has been a malfunction of the ACS. The TSA also needs to be notified of the changed condition and approve the alternate measures.

Other airports have taken a more detailed approach to establishing their EAAs. These EAAs make explicit some provisions that are only implied in the more generalized agreements. As an example, a more detailed EAA might include provisions like outlining post responsibilities, general staffing levels, and/or patrol requirements or policies. These agreements include details of security arrangements that are not expressly provided for in Part 1542. An example of a detailed EAA table of contents is attached as Appendix B.

[6] 49 CFR § 1542.107(a)

Most airports that authorize EAAs retain control over badge issuance. However, this function may be passed onto the tenant in the EAA. For example, some airport EAAs have included provisions for tenant issuance of badges for the SIDAs controlled under the EAA. The exercise of that function is audited and controlled by the TSA. The issuance of tenant badges for access in tenant-controlled SIDAs requires the tenant to support an equivalent capability to the airport's badging capability. Criminal History Records Checks (CHRC) and Security Threat Assessment (STA) requirements apply to the ID media issued for unescorted access. The research revealed that the issuance of tenant badges required the development of procedures for the acceptance of both tenant- and airport-issued media within the tenant-controlled SIDAs. Provisions were also made for airport issuance of badges to those tenant personnel needing access to those SIDAs of the airport outside of the boundaries of the EAA area.

One airport has created an EAA that requires the tenant to provide details of security staffing arrangements and practices for tenant-controlled areas. Other airports handle these matters through requirements for positions to be staffed and security procedures to be established.

One large airport has created an EAA template for use in multiple EAAs. Most other airports negotiate EAAs on a case-by-case basis. In some instances, airports have different operating arrangements for similar tenant operations; for example, one tenant with an EAA and one without. There is no one-size-fits-all approach for airports based on size or facility type under consideration.

Establishment of an EAA creates a "need to know" on the part of the regulated entity, so that the SSI information relevant to Part 1542 compliance can be provided to the tenant. A process should be put in place to ensure that the information is available to the tenant and the contents remain secure. Guidance for protecting SSI is available from TSA.[7]

Many airport operators favor EAAs because EAAs place security responsibility directly and explicitly on the tenant instead of the airport. EAAs are thought to help maintain good relations with the TSA, and minimize the airport's exposure to any financial burden resulting from violations and fines. While the EAA does place responsibility directly on the tenant, there is no express provision in Part 1542 that specifically excludes the airport from liability if the EAA conditions are met. There are also no provisions requiring an airport to maintain a certain level of oversight, although any change of conditions that necessitates the tenant to implement alternative security measures is required to be reported to the airport. It is unclear whether some degree of airport oversight is required or if the TSA could levy penalties against the airport if it is found that an incident could have been avoided with proper oversight. For this reason, it is important for airports to maintain some measure of oversight, even where there is an EAA, to help ensure tenants are fulfilling their responsibilities. Failure to do so could result in a security event or the airport receiving a notice of violation from the TSA.

The airport should ensure that there is an option to terminate an EAA through the routine ASP amendment process. The termination process should address terminations for the convenience of the airport or for instances where the tenant is unwilling or unable to meet compliance requirements. The TSA has recommended that airports conduct annual reviews of their EAAs for compliance and applicability; these reviews should be documented in writing.

EAAs should also include an acknowledgment that TSA reserves the right to cancel the EAA at any time if it is determined to be in the interest of airport safety and security based on a TSA evaluation of compliance.

[7] https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf

Tenants with EAAs may allow other aircraft operators or foreign air carriers to use the area covered by the EAA. However, the tenant retains responsibility for security compliance by all users. The responsibilities outlined in an EAA cannot be shared among aircraft operators or foreign air carriers. Security requirements that are not transferred to the tenant in the EAA remain the responsibility of the airport.

It should also be noted that law enforcement responsibilities cannot be delegated or included in an EAA; those must remain with the airport operator.

3.1.2 ATSPs

ATSPs are authorized under 49 CFR § 1542.113 and, unlike EAAs, they can be executed with unregulated parties.[8] The use of ATSPs is not commonplace. In fact, the research failed to find evidence of a single TSA-approved ATSP. However, two airports that were pursuing ATSPs shared their draft agreements with the research team. These drafts offer some insight into the types of measures that may be included in an ATSP.

ATSPs are more expansive than those of EAAs, and necessitate more airport involvement and oversight. Requirements include:

- The ATSP applies to tenant leasehold areas, and responsibility must be exclusive to one tenant
- The exclusive area cannot be shared and cannot apply to areas in the passenger terminal
- The airport tenant must undertake the provision of security for the designated portion of the Secured Area,[9] AOA,[10] and SIDA[11] over which they maintain exclusive control.
- The tenant may not assume law enforcement responsibilities and TSA must determine that the tenant is able and willing to meet the requirements of the ATSP
- TSA reserves the right to amend or terminate the ATSP[12]
- Access points to areas that are exclusive to the tenant in the ATSP need to be identified within the agreement, along with provisions for securing them
- A provision needs to be included in the ATSP for notification in the event of changed conditions, including the implementation of alternative security measures
- The ATSP must describe, with sufficient specificity, the measures that demonstrate the tenant is capable of carrying out security requirements in the same fashion as the airport operator would

An ATSP will likely require TSA headquarters-level approval before acceptance. TSA will examine the tenant's ability to manage security practices. This type of evaluative process is not extended to tenant participants of an EAA, likely because EAA participants are already regulated entities. In reaching that determination the TSA will consider:

- The location of the tenant facility
- The tenant's relevant knowledge of security operations and requirements
- The tenant's relevant capabilities to perform those operations and meet requirements

[8] Tenants other than those regulated under 49 CFR § 1544 or 1546
[9] 49 CFR § 1542.201
[10] 49 CFR § 1542.203
[11] 49 CFR § 1542.205
[12] 49 CFR § 1542.105

With respect to assessing the relevant knowledge and capabilities of the tenants, it is advisable that the security requirements be detailed with great specificity. This is particularly important because an ATSP tenant is a non-regulated party with limited access to TSA requirements that may be found in regulatory sources (e.g., Security Directives, National Amendments, Information Circulars, etc.) The airport should be careful to ensure that all requirements are well understood and that there is a clear process to both advise the tenant regarding changed requirements and ensure tenant compliance. The ability of the tenant to adapt to those changes is part of the TSA's evaluation.

Establishment of an ATSP creates a "need to know" on the part of the tenant. The ATSP must include provisions to protect SSI in accordance with the 49 CFR § 1520. This should include an indication that people entrusted with SSI are subject to civil fines and penalties for improper SSI disclosure.

ATSPs are not tenant leasehold agreements, and such arrangements do not create ATSPs. Entry into an ATSP must be a voluntary action on the part of the tenant. Only tenants can enter into ATSPs—not contractors who are not tenants—and multiple tenants cannot be party to a single ATSP.

An ATSP differs significantly from an EAA with respect to requirements for airport monitoring and audit of tenant activities. It also differs in that an ATSP requires the airport to implement provisions for monetary fines and penalties for non-compliance, and provisions for termination. The penalties should be on an escalating scale, and the airport needs to provide a process for contesting those penalties.

The ATSP is also required to include a detailed description of how the airport will audit and monitor ATSP compliance. The airport's role in auditing and ensuring ATSP compliance is similar to the TSA's role in auditing and ensuring compliance of EAAs. This would generally require a program of inspections, interviews, observations, and records reviews. However, in addition to supervision by the airport, the tenant is also subject to inspection by the TSA.[13]

If the TSA determines that a tenant under an approved ATSP or its employees, permittees, or invitees are non-compliant with the agreement terms, the airport will be excused from liability for the regulations and penalties for that non-compliance. Such an express grant excusing airport responsibility under Part 1542 is not found with EAAs. In the event of ATSP-tenant non-compliance, TSA will take immediate action to ensure that the non-compliance is remediated, and the airport will be responsible for ensuring the required corrective action is taken. However, if the airport cannot demonstrate that it has performed its monitoring and audit responsibilities or supervised redress for tenant non-compliance, the TSA may cite the airport. In support of assertions that it has complied with its responsibilities under the ATSP, the airport should be prepared to produce records of audits and the corresponding results, assessments, and penalties assessed against the tenant for non-compliance.

The ATSP must contain provisions indicating causes for termination of the agreement, including but not limited to failure to comply with security measures. It must also contain provisions for immediate notification, and provide alternative security measures in response to changed conditions.[14] The airport is responsible for taking appropriate action for tenant non-compliance, including the imposition of monetary and non-monetary penalties. Should the airport fail to do so, the TSA has the authority to terminate the ATSP and assess penalties against the airport, the tenant, tenant employees, and other accountable people.

While tenants can employ private security, the ATSP cannot transfer law enforcement authority to the tenant.

[13] Part 1542.5
[14] Part 1542.103(a)

During the research, two airports shared ATSP templates and indicated they were pursuing TSA approval of ATSPs at their airports. One template reserved the responsibility and authority for badging of Secured, AOA, and SIDA access to the airport. The second template had a more limited agreement, though it provided for tenant badging of personnel for Secured Area, AOA, and SIDA access. The tables of contents for these agreements are provided in Appendix B.

For airports that act as a base of operations for non-regulated cargo carriers, such as Amazon Air, an ATSP may be a viable option. Many larger, non-regulated entities have the ability to control their own security measures to meet the TSA and airport's standards through the use of an ATSP.

3.2 Ad Hoc Federal Regulation

EAAs and ATSPs have defined requirements under federal regulations, but other arrangement types can also have federal oversight and compliance. Including tenant measures in an ASP, or appending tenant security agreements to an ASP will trigger federal oversight over security measures. There is, however, no set template for these measures, and no assurance that federal enforcement activity will be directed against the tenant and not the airport.

3.2.1 ASP Provisions

The most common way for airports to enforce security compliance at tenant facilities is through the general security provisions of the ASP. These provisions are made applicable to the tenant through two different processes: (1) directly through the credentialing process that allows for unescorted access to specified areas of the airport where the tenants operate, particularly the Secured Area, AOA, and SIDA, and (2) indirectly through reference to the ASP or federal regulatory compliance in documents like leases or rules and regulations concerning airport properties. Some airports have sought to augment the more general provisions of their ASPs by executing tenant security agreements, which they sometimes include in their ASP. While not formally recognized under 49 CFR § 1542, these agreements are often prepared and executed with approval by TSA under their role as regulator of federally required ASPs.

The TSA has discretion in how it enforces security at airports. In some instances where TSA is satisfied with airport security practices and enforcement measures, the TSA may focus enforcement efforts on the tenant or tenant's employees, permittees, and invitees, rather than the airport. While this shift in focus is not dictated by regulation, it seems to be a fairly routine TSA practice in many airports, particularly at airports that develop more robust security programs for tenants, either directly in the ASP or through TSA-approved tenant security programs.

The ASP does not afford the airport the ability to levy fines and penalties against individuals and companies. Nor does it enable airports to shift responsibility for fines imposed by TSA on the airport for tenant noncompliance. Airports with tenants that have a history of security violations should ensure that their leasing agreements or airport rules and regulations allow for enforcement of the security measures in the ASP. These agreements would allow the airport to more closely monitor the tenant's security-related activities and levy penalties for non-compliance, in addition to any measures TSA may impose. Non-regulatory measures, such as leases and airport rules and regulations, are utilized almost universally to enforce compliance with security requirements in the ASP.

3.2.2 Other Tenant Security Arrangements

As a result of the challenges and requirements of creating EAAs or ATSPs, and rather than simply relying on general provisions of their ASP, many airports have chosen to develop their own tenant

security arrangements. These agreements are commonplace in airports, even when the airport chooses to execute an EAA with some tenants. Because these agreements are not created through federal regulation, they can be made applicable to both regulated and non-regulated entities.

The names of the documents or programs vary by airport—to include Alternate Security Measures and Tenant Access Control Program, among others—but most of the agreements roughly parallel the contents of EAAs. Typically, they include provisions for:

- Access control procedures at all AOA, Secured Area, and SIDA access points
- Challenge procedures
- Escort procedures
- Signage and notice requirements
- Training requirements
- Changed conditions procedures
- Special circumstances
- Notice procedures
- Identification of contact persons

Since these agreements are not subject to any specific regulatory requirements, airports and tenants are free to include any provisions they desire and that are permitted by their state and local authorities. However, airports should be mindful that the EAA requirements are a bare minimum that TSA would expect to establish a secure environment for SIDA access and control, at least for the operations of a regulated party. Thus, the closer the agreement adheres to those minimum requirements, the more likely it is that the TSA will embrace the provisions as a primary basis for enforcement against the tenant. On the other hand, both the airport and the tenant should be mindful that the more provisions that are incorporated into the ASP, the greater the exposure of both parties to TSA regulatory action for noncompliance. Examples of security agreements of varying detail are provided in Appendix C.

As with the incorporation of tenant security provisions directly in the ASP, the use of these other security arrangements does not compel the TSA to hold the tenant primarily or exclusively accountable for violations, or otherwise excuse the airport of responsibility or liability for tenant noncompliance. Enforcement practices are within the TSA's discretion, so understanding the position of local TSA with respect to enforcement is an important part of the decision to enact these procedures.

Most of the tenant security arrangements used by airports were location-based and focused on the area occupied by the tenant leaseholder. However, one airport focused their tenant security plans on an operations-based program because the tenant was operating in areas that they did not exclusively occupy at all times. The requirements of the operational tenant agreement were activated during operational periods and deactivated at their conclusion. Specific, measurable processes were laid out for activation and deactivation and enhanced tenant security measures were only required during the period of activation. A detailed outline of this agreement is provided in Appendix C.

3.2.3 Exceeding Regulatory Requirements

Some airports, in an attempt to increase security, use their ASPs or other security agreements to impose requirements that exceed the 49 CFR § 1542 requirements. However, this can cause tension for some tenants operating their own facilities on airport property—especially those that operate out of several airports. These tenants are generally very familiar with the requirements in Part 1542, and have modified

their operating processes to meet these requirements. To avoid potential confusion, airports that go beyond Part 1542 requirements should work closely with their tenants to help them understand how the changes affect them and their operations.

In addition, the introduction of measures in the ASP beyond those specifically required by Part 1542 has the effect of increasing federal regulatory compliance requirements for both the tenant and the airport. Many airports are deterred by the additional compliance requirements and therefore avoid adding measures to their ASP beyond those specifically required in Part 1542. For those airports, it is important to recognize that creating additional measures in the context of a tenant security agreement may have a similar impact in increasing compliance requirements.

Rather than relying on enforcement directed through the TSA in relation to the ASP, many airports focus compliance efforts through enforcement of local rules and regulations, or through the use of lease provisions. These mechanisms allow for airport action without relying on federal input or efforts. The enforcement can be focused on a specified violation of an airport rule or lease term. Often, both rules and regulations and lease provisions provide that a violation of a federal security regulation or ASP term is an independent violation of an airport rule or lease. This allows for enforcement by either the TSA or the airport, or both entities. More detailed information on this approach can be found in Section 3.3, Non-Federal Measures.

3.3 Non-Federal Measures

In addition to federal compliance enforcement measures, airports have other tools at their disposal. Local regulations are commonly used to address security measures. The language from these regulations, as well as federal regulations, are frequently incorporated directly or by reference in lease agreements. Licensing tenant personnel operating in airports is another, newer approach. These measures are outlined below.

3.3.1 Lease Agreements

For most airports, airport-use agreements and lease agreements mandate tenant compliance with applicable security requirements outlined in federally regulated security documents, such as the ASP. This may involve general reference to federal regulations or reference to airport-specific security plans.

Because they are often long-term arrangements, in some cases up to 99 years, leases may involve substantial legal processes to change or modify. They often require the approval of airport or county boards or city councils. Accordingly, adjustment of leases to deal specifically with changing federal security regulations may be cumbersome and difficult. It is advisable to reference categories of regulations, such as “federal airport security regulations,” rather than specific regulatory provisions, such as a 49 CFR § 1542 provision. This language may reduce the need for lease agreement amendments when federal security requirements change.

Leasehold and user agreements can and do carry enforcement provisions with respect to violations of the agreement. Those can include indemnity, specified penalties, general damage remedies, and liquidated damage provisions. For example, some leases require the tenant to pay any fines or penalties levied against the airport as a result of the conduct of the tenant or any person utilizing the tenant’s leased property as an invitee or permittee. The airport should understand that penalty provisions in a lease can only be asserted against parties to the agreement.

Lease agreements can provide for termination in the event of significant non-compliance. Additionally, they can allow for the airport to remedy any security deficiencies on the tenant’s lease property, and

allocate the costs of those remedial measures to the tenant. These "self-help" provisions generally require notice to the tenant, allowing them to remediate deficiencies, but ultimately afford the airport the right to act if the tenant fails to do so promptly. The timeline for tenant action may be compressed if the deficiency constitutes a dangerous condition that requires immediate attention. The cost allocations for remediation would not be considered a fine or penalty, but more in the nature of an addition to rent. Airports may also seek to impose these self-help provisions under their rules and regulations.

Airport counsel should be involved in any decision to use a lease as a mechanism of enforcement, as it will involve legal issues and may lead to litigation.

3.3.2 Rules and Regulations

Airport rules and regulations are another source of authority for managing tenant security. Like lease agreements, rules and regulations almost always contain general reference to federal regulations or airport-specific security plans enacted in accordance with federal regulations. They may also reference specific offenses, such as lost badges or access control violations, often in conjunction with their corresponding penalties.

Like leases, the provisions of rules and regulations tend to be long-term arrangements. While they can be changed unilaterally by the governmental entities that created them, they are generally not subject to rapid or frequent change, and involve specified governmental processes to modify. Often the processes for publishing or modifying rules and regulations can be lengthy and cumbersome for the airport. Additionally, these actions may be outside the airport's direct control, as they may require approval of a city council or county board.

Enforcement of airport rules and regulations is outside of the purview of the TSA, although they frequently specify offenses that may also be the subject of federal regulations that are enforceable by the TSA. For example, most regulations have some form of provision against unauthorized access. Similar provisions also appear in federal regulations, as well as in regulated ASPs, EAAs, and ATSPs. Non-compliance can result in separate proceedings brought by the airport under airport rules and regulations and by the TSA under federal regulations.

Rules and regulations require the establishment of some sort of due process provisions. After a citation, there is generally a hearing by an independent hearing officer, as well as for some sort of additional review of fines or penalties imposed. Those procedures vary widely by state and local governance. Unlike leases, rules and regulations can direct penalties at tenants, their employees, contractors, and suppliers—essentially, any person or entity operating on airport property. Thus, a penalty can be imposed directly against the person committing the infraction and not just the tenant organization. Depending how the rule or regulation is written, both parties could be simultaneously liable.

3.3.3 Licensing/Certification Programs

Some larger airports have developed and implemented airport licensing/certification programs. These programs certify companies and their employees—including airport tenant facility operators and their employees—for operation on airport property. They are generally part of a permit authorizing tenant work on airport property, and can be operated independently of or in conjunction with lease requirements. The programs ensure a sufficient level of training for all personnel working on the airport who may or may not be employed by a tenant organization. In constructing these programs, airport security should work closely with properties, facilities, maintenance, and concessions management departments at their airports.

The programs often include concessionaires, vendors, and construction personnel, and outline minimum standards in the following areas:

- Airport security
- Vehicle and equipment safety
- Experience and capacity requirements for services in certain areas of the airport
- Property and facilities orientation
- Emergency response procedure awareness
- Personnel and training requirements
- Orientation regarding standard use terms and conditions of leases

The licensure programs feature training for individuals who will work in the airport environment. This offers an opportunity to stress the importance of security practices for the entire airport community, as well to enforce compliance standards for security regulations. Failure to comply with security requirements may result in enforcement of individual and organizational non-compliance penalties, such as suspending privileges or imposing monetary fines.

3.4 Credentialing

It is difficult to overstate the importance of credentialing in the enforcement of tenant security practices. To ensure security requirements are taken seriously, airports frequently impose sanctions on persons for noncompliance with security measures. Those sanctions include monetary fines and badge-related penalties, such as the suspension or termination of badge privileges.

In circumstances where airports permit the tenant to issue its own ID media, airports should ensure that the agreement places requirements on the tenant that align their process with the airport's credentialing requirements. This type of arrangement would be limited to EAA and ATSP areas. Moreover, those agreements should discuss the use of airport-issued ID media in tenant areas, and the need for some tenant employees to have airport-issued media that allows access to regulated areas outside the EAA or ATSP footprint. Agreements should never permit access to regulated areas of the airport outside the tenant's exclusive control (EAA or ATSP) without airport-issued or flight crew media.

3.4.1 Communicating Security Requirements

The ID media issuance process for unescorted access presents an opportunity to communicate security requirements to tenants and their personnel. It offers the opportunity to highlight security concerns that may or may not be contained in an agreement with the tenant. As an example, the security orientation for many airports includes training on issues such as the importance of preventing unauthorized access, reporting of unusual events or incidents, challenge procedures, and escort practices. Tenant security programs should be aligned with the training objectives and requirements in the airport credentialing process.

Reliance on the credentialing process for security education does have limitations. For example, this training does not apply to persons who are not issued ID media, which may leave many people working in public areas in proximity to restricted areas without adequate security orientation. Additionally, airports that allow for tenants to operate EAAs or ATSPs should consider imposing training requirements in conjunction with the tenant badging process.

The credentialing process also provides a direct communication channel to tenant organizations through Authorized Signatories. These individuals are responsible for managing an organization's requirements

in the airport credentialing processes. Authorized Signatories reinforce security messages between the airport and the tenant employees.

3.4.2 Utilizing Authorized Signatories

Airports using a leasing agreement should make sure that Authorized Signatories are well-trained in the security responsibilities outlined in the ASP and are communicating the airport's security expectations to their employees. Typical lease agreements only have general language directing the tenant to comply with the federal regulatory measures, such as the ASP, but tenants do not typically have access to view the ASP as it is an SSI document. Using the Authorized Signatories, airports have an established communication path to convey and reinforce required security practices to tenants without granting access to the entire ASP. While all training in connection with ID media issuance provides information regarding individual employee responsibilities, Authorized Signatory training often has a more in-depth treatment of the responsibilities of the tenant. For this reason, these training sessions are also a useful method of disseminating information necessary to ensure tenant compliance.

While special training may be required for some tenants, like those with ATSPs and EAAs, the Authorized Signatories can be a useful conduit to provide or supervise tenant training requirements. If using Authorized Signatories, it is important to understand they are often administrative personnel, not managerial, and may have limited authority. Considering this, airports should recognize that some compliance matters may require attention from a higher managerial level in tenant organizations.

SECTION 4: CRITICAL FUNCTIONS OF THE AGREEMENT

Regardless of the compliance mechanism, several critical security functions should be addressed in the agreement between the airport and the tenant. These include access control, security personnel, security practices, ID management, challenging, escorting, inspections, audits, notifications, and sanctions. The level of detail describing these functions and their requirements varies based on the type of agreement, as well as the approach the airport chooses to take with the individual tenant.

This section includes a discussion of the various security functions that airports might wish to consider including in tenant security agreements. Some of these functions may be required by EAAs and ATSPs, but are completely discretionary for other agreements. After the discussion in each section, examples of language addressing those concerns are provided. The excerpts of language appear in gray boxes with any changes from the original appearing in **blue**. The language is taken directly from a variety of sources, including EAAs, ATSPs, other tenant agreements, leases, and rules and regulations from airports of varying sizes. The type of arrangement the language was taken from and size of the airport is noted for each excerpt.

The sample language is not meant to be comprehensive for every possible scenario an airport may encounter. Airports considering this language are encouraged to adapt these samples to their own needs and requirements.

Airports using the sample language in their own agreements should consult their airport legal department to review the document.

4.1 Access Control

Access control requirements include procedures for permitting and safeguarding access, as well as the physical ACS (i.e., automated systems, lock and key systems). This section covers the policies and procedures for permitting access and maintaining access control. The issuance of ID media, which is frequently related to automated access control, is also addressed in this section. The operation of the ACS is discussed in Section 6, Infrastructure and Equipment to Support Tenant Security Programs.

The requirement for establishing access control is commonly adopted in all agreement types, and usually outlines the responsibility for access control points and their maintenance. However, language that specifically addresses the process at a specific access control point is often lacking. This is most likely because airports use a variety of physical systems and technologies to support the access control measures. Sometimes those differences are even found within the same tenant area.

Most agreements addressing access points rely on maps and diagrams to indicate the access points and gates. Sometimes a door or gate chart is attached, indicating the use of a particular access point and the type of access control measure used to secure the portal. Example control measures include automated access control, key and lock, and cipher locks, among others.

The centralization of automated ACS allows airports to have a highly accurate picture of who is entering the restricted areas of the airport. While a centralized system operated by the airport seems to be the preferred model, most airports do not have such a system installed at all access points, as it is not always feasible. In some instances, the infrastructure requirements, particularly cabling and power, prohibit such solutions. In other instances, tenant preferences for a system they can control—particularly in the cases of agreements like EAAs—result in the creation of a standalone ACS.

Tenant facility doors—even those that access restricted areas of the airport—often have separate tenant-operated ACS. However, at least one large CAT X airport included all access portals leading to restricted areas in its automated ACS. A fully automated system controlled by the airport offers the prospect of a single procedure for access to any portal. It also ensures that authorized airport personnel can access any tenant area. In locations where access is controlled by a tenant system, separate arrangements need to be made to enable access for selected airport personnel, such as airport security and operations.

Typically, access through vehicle gates, which often lead to common areas, is controlled on a centralized ACS. However, when the gate is exclusively accessed by one tenant area, it is often operated with tenant-controlled system. With respect to gate access control, the most common factor in who maintains control is the cost and physical ability to include the gate in the airport's systems. In instances where cost or feasibility is an issue, the tenant facilities are not on a centralized automated ACS. Automated access control at those facilities, if it exists at all, is typically installed and operated by the tenant. Most tenants prefer to maintain exclusive access control for their critical facilities.

Most airports choose to retain the responsibility for issuing access media to tenant personnel for unescorted access in regulated areas. This enables the airport to maintain control over tenant badges as well as each individual's scope of access. In instances where tenants maintain their own automated ACS, separate access control media must be issued by the tenant. Typically, these are issued as company ID badges.

In some EAAs where tenants were authorized to issue their own ID media for access to tenant-controlled regulated areas, access for airport personnel became an issue. This typically occurs for operations and security personnel who need access to tenant-controlled areas, therefore a solution needs to be addressed in the agreement with the tenant. Often, this may require issuing access credentials for the tenant system to selected airport personnel. Similarly, in instances where tenant employees require access to regulated areas of the airport outside of their footprint, those individuals will require airport-issued access media.

Tenant-managed physical access control within tenant facilities may complicate some airport operations. In airports where EAAs are operated in congested areas, managing dual badge access will add an administrative burden because of the larger number of persons requiring dual access, as well as the larger number of circumstances requiring access. Identifying the people and circumstances for which dual access is needed requires coordinated planning by both the airport and EAA tenant. The physical EAA facilities in more easily segregated or remote areas of an airport footprint tend to have fewer problems with respect to application of access control measures.

One compelling reason for affording physical access control responsibility to tenants operating out of their own facility is that they may have high turnover rates in their worker populations. This can create a significant burden on the airport credentialing office if they are required to issue and maintain the access media of the tenant's workers in the event of a centralized ACS. Most tenants operating their own facility manage the issuance of their own media for access to those facilities. This is often in addition to ID media issued by the airport for individuals requiring access to adjoining regulated areas; however, since not every worker will need such access, the burden on airport credentialing staff is still reduced.

If the airport must manage the access media of the tenant, consideration should be given to allowing Authorized Signatories the ability to deactivate a badge directly in the event of a worker quitting or being fired. This would lessen the burden on the airport credentialing office, and ensure timely deactivation of access control media.

As a measure to manage access into regulated areas, airports should consider working with tenants and TSA to re-establish airport boundaries to minimize the number of tenant workers needing unescorted access. Also, when building new facilities, it is ideal to position them outside of the airport regulated-area boundaries. These options would allow the tenant to maintain their own access media, limit the number of people accessing the airport-regulated areas, and reduce pressure on airport credentialing offices.

As the schema to manage access to regulated areas is developed, the airport should consider ways to ensure that changes in federal regulatory requirements, security imperatives, and tenant operational requirements are planned for. The use of a regular audit program should be considered to ensure that any of these changes are accurately documented in security plans and reflected in security practices. The process of documenting changes requires a clear communication path between the airport and tenant to ensure that changed requirements are properly documented and applied.

SAMPLE LANGUAGE

The following language outlines tenant responsibilities and airport access rights where tenants maintain access control.

Language on General Access Control Responsibilities

This language is taken from Alaska Department of Transportation (DOT) regulation. Alaska DOT manages a large network of CAT III airports based on state law and state-approved lease templates. Other state-operated airports are controlled by different code sections. The provisions below require tenants with leaseholds adjacent to restricted areas, like SIDA, to control unauthorized access. It also affords the state the right to enter into the leasehold property to construct barriers necessary for security. Those barriers must then be maintained at the tenant's cost and expense.

Restricted areas and access to restricted areas.

(a) The department may enter onto a premises to erect or to maintain a barrier if the department determines that a barrier is necessary for safety or security at the airport. Except in the case of an emergency or threat to public safety, the department will give advance notice to a lessee, permittee, or concessionaire before erecting a barrier on the lessee's, permittee's, or concessionaire's premises. To the extent practical, the department will erect the barrier in a location where the barrier will not disrupt the operations of the lessee, permittee, or concessionaire. The lessee, permittee, or concessionaire shall thereafter repair, reconstruct, or replace the barrier on the premises to the satisfaction of the airport manager at the lessee's, permittee's, or concessionaire's sole expense if the barrier is damaged or rendered ineffective for its intended purpose as a result of activities of the lessee, permittee, or concessionaire or an agent, contractor, or invitee of the lessee.

(b) If the premises of a lessee, permittee, or concessionaire is within or adjacent to a restricted area, the lessee, permittee, or concessionaire shall ensure that only authorized persons enter or remain in the restricted area.

Language governing access control is also common in regulation by county or city ordinances as part of broader regulatory schemes that govern a range of airport activities. The provisions below are part of a broader ordinance that governs activities at a county-operated CAT I airport. Those provisions include regulation of ID media issuance and use, responsibilities of authorized persons, violation reporting requirements, and a delineation of prohibited acts.

County Airports

Responsibility of airport tenants.

1) Adherence to the security ordinance. Airport tenants with access to airport security areas on their property shall follow this ordinance by posting signs approved by the county, which prohibit access leading into airport security areas.

2) Preventing unauthorized access to airport security areas. Airport tenants with access to airport security areas shall at all times keep the access secured or staffed in a manner that prevents unauthorized persons from accessing airport security areas. Tenants shall retain keys or other means of access to airport security areas under their control and issue such access only to authorized persons.

3) Appoint security contact. Airport tenants with access to airport security areas shall appoint at least one employee of the airport tenant as the security contact primarily responsible for the airport tenant's leased area which accesses airport security areas. Airport tenants shall advise the airport security coordinator in writing of the person or persons at all times having such responsibility.

This language from a CAT I airport takes a general approach to citing the airport's rules and regulations, and then offers more detailed description of control over tenant areas in individual facility access plans. This language lays out responsibilities for notice using signage, and the requirement to safeguard keys.

Security Responsibilities

The County has the overall responsibility for law enforcement activities of the Airport. Operators, Lessees, or Sublessees are responsible for the security of entity's Leased Premises and shall comply with the airport management's security requirements.

Airport tenants with access to Airport security areas on their Leased Premises shall comply with these Rules and Regulations by posting signs approved by the County, that prohibit access leading into Airport security areas.

Airport tenants with access to Airport security areas shall at all times keep the access secured or staffed in a manner that prevents unauthorized persons from accessing Airport security areas. Tenants shall retain keys or other means of access to Airport security areas under their control and issue such access only to authorized persons.

This provision from a CAT I airport's tenant security program contains an acknowledgment by the tenant for access control responsibility within specified areas. This provision is in addition to measures required by 49 CFR § 1542.

Tenant is hereby delegated, and accepts, the authority and responsibility to control access to the AOA and SIDA, which for the purposes hereof is defined as those portions of the Airport provided by the Authority for aircraft and related operations, and shall include runways, taxiways, aircraft ramps, aprons and any portion of the Airport required to be enclosed by security fencing under Federal Aviation Regulations. In carrying out such authority and responsibility. **Tenant** agrees that it shall, at a minimum, implement and maintain the following security measures.

Tenant assumes sole responsibility and liability for all access to and from the AOA and SIDA through the Gates and Doors while they are in use by **Tenant** or any of its representatives, and shall prohibit the entry of unauthorized personnel into the AOA and SIDA. At all times while not in actual use, the Gates and Doors shall be locked for the control of the secured areas.

Language on Identification of Access Points

Identification of access control points is usually addressed in an ASP, EAA, ATSP, or Tenant Agreement. The figure below is an example from the Tenant Agreement from a CAT II airport that delineates the access points in a tenant area.

Tenant Doors and Gates

Door #	Location/Activity	Type	Method of Control

Type: PD – Pedestrian Door, PG – Pedestrian Gate, OH – Overhead Roll-Up Door

Method of Control: TKS –Tenant Key, TSCAS – Tenant Security Computer Access Control System, CIPH – Cipher Lock, TCL (Tenant Chain/Lock) – Chain and Padlock with Tenant Key

The following chart is taken for the Tenant Security Program of a CAT X airport.

Door Name/Description	Door Location	Control Measures	Who Has Access	Monitoring
Door 1/ Pedestrian	Main entrance to the building	Company card reader, push button by receptionist	All visitors	CCTV
Door 2/Pedestrian	Door from office space into the hangar	Company card reader	Staff with **XXX** AOA badges only	

Language on Site Surveys of Access Points

This language from a CAT X airport EAA requires the tenant to prepare and submit a site survey. Use of maps and site survey documents are not uncommon requirements for identifying the locations of access points. This language could be adapted for non-EAA airport agreements where the tenant is responsible for the security of access points.

Tenant shall provide the **Airport** a site survey of access points. The survey shall be on an 8 x 11-inch format. Any changes to these points shall be immediately forwarded to Airport Security.

4.2 ID Management

ID management is the process of verifying identity and granting unescorted access to regulated areas. The issue of ID media is often related to automated ACS, but that is a matter of convenience, not a requirement. In most airports with a centralized ACS, the ID media is also the access media. Even where there is no centralized automated ACS, most airports have maintained centralized control over identity

management related to granting unescorted access to regulated areas. Most tenants, however, maintain identity management rights over those individuals that can access their facilities.

Where tenant populations are extremely large, there can be some advantage in allowing the tenant to perform some or all of the ID management functions for their employees. Tenants that are regulated entities[15] maintain their own identity management processes, and sometimes those processes are utilized in connection with airport ID media issuance if the airport accepts the results of air carrier background checks. With respect to some EAAs, the Part 1544 badging process is utilized to create badges with access to the regulated areas outlined in the EAA.

ID media issuance by non-regulated parties has not yet been addressed by TSA, so the applicability of this approach to an ATSP is not yet clearly established.

Instances of airports authorizing tenants to issue ID media almost exclusively involved large cargo carriers. The common denominators among airports' authorizing tenants to issue ID media included:

- Required access for a sizable number of airport-based tenant personnel
- A footprint of tenant facilities and operations in a clearly separable and remote area of the airport
- The tenant had proven to be capable of performing background screening and badging employees

In cases where the tenant was permitted to issue badges for SIDA access within the EAA footprint, measures needed to be taken to allow for access by selected airport personnel, principally security and operations personnel. Measures also had to be taken to allow for airport ID media issuance for tenant personnel who may need access to regulated areas of the airport outside the EAA footprint.

SAMPLE LANGUAGE

The language below addresses ID media issuance and use in airports. It addresses the importance of ID media as a security measure and a token that is also often used in conjunction with automated ACS. Airports can consider adding this language to EAAs, ATSPs, or other tenant agreements to manage ID media accountability and control.

General Language on ID Media Issuance

This language from the rules and regulations of a CAT II airport provides a concise exposition of the badging process for access to SIDA and the AOA. This schema addresses only airport-issued ID media. Tenant-issued ID media is not permitted at this airport.

The access badge required for unescorted access to the AOA will be obtained from the Airport Authority via the Badging Office. To receive such access, TSA required checks, including a security threat assessment, a criminal history background check and fingerprint check, will be performed as required. Badge holders will agree to comply with TSA regulations and the Airport Authority Airport Security Program.

Unescorted Access; Air Operations Area (AOA)

Unescorted access to the Air Operations Area is limited by badge type and color.

RED: Access is approved in all areas of the AOA and Secured Areas.

WHITE: Authorizes unescorted access to Sterile Area ONLY.

BLUE: Authorizes access to the Secured Area, Sterile Area and AOA Non-Movement Areas.

GREEN: Authorizes access to the AOA Movement and Non-Movement Areas, excluding the Secured Area.

[15] 49 CFR § 1544

Red/White/Blue: Authorizes access to AOA Non-Movement Areas only, excluding the Secured Area.
"D" –designation: Authorizes vehicle gate access and motor vehicle usage.
"X" –designation: Not authorized to escort others.

This language from the rules and regulations of a CAT II airport provides a concise statement of roles and expectations regarding the issuance of ID media.

Control, Use and Display of Airport Access Control Media

a. All access control media are the property of the Airport Authority and as stated on the badge must be immediately surrendered to the Airport Authority upon demand.
b. Access control media authorizing access to the Movement Area or Secured Area must be continuously displayed on the outermost garment, above the waist, while within the Movement or Secured Area and whenever instructed by the Airport Authority.
c. Access control media which allows access to non-Secured and Non-Movement Areas only must be in the possession of the authorized badge holder at all times while within those areas and must be produced upon challenge.
   - Access control media shall be kept current and in such condition to make visual identification certain and is the holders responsibility to replace if necessary and at the owners expense. Access control media is available through the Badging Office (**XXX-XXX-XXXX**).
   - Access control media are issued for individual use only and shall not be borrowed from another and shall not be loaned to another for any reason.
   - Loss of access control media shall be reported immediately and without delay to the Dispatch Center (**XXX-XXX-XXXX**) and/or Badging Office (**XXX-XXX-XXXX**).

Language on Tenant ID Media Issuance

The issuance of ID media by a tenant is permissible for EAAs—though the practice is not required or commonplace. The language below for ID media issuance for unescorted access is taken form the EAA of a CAT I airport.

Carrier Badging Procedures. Carrier has been granted authority under this Agreement to issue Identification Badges **("Carrier Badges")** to its employees and contract employees seeking unescorted access to the Secured Area, AOA and/or SIDA in Carrier's Exclusive Area.

If Carrier has been granted authority pursuant to this Section [of this Agreement] to issue Identification Badges, the Carrier shall comply with each of the following requirements:

- Carrier shall certify to the Airport that it has complied with 49 CFR §1544.229 for each such employee and contract employee issued a Carrier Badge and shall provide the Aviation Security Manager with updated lists of badge holders on a monthly basis.
- Each Carrier Badge shall meet the requirements set forth in 49 CFR §1542.211 and shall be in the form set forth in Exhibit E.
- Each individual issued a Carrier Badge shall be trained, at a minimum, to comply with the requirements of this Agreement, as set forth in Exhibit G, including without limitation the following:
  a. Proper display of Identification Badges;
  b. Challenge procedures as set forth in Section 6.4;
  c. Escort procedures as set forth in Section 6.5; and
  d. Limitation on a badge holder's unescorted access authority.

The language below for tenant issuance of ID media allows for unescorted access to tenant areas, and is taken from the EAA of a CAT I airport. The interrelation between those badges and ones issued by the airport authority is outlined here.

The **Tenant** badges that are based on CHRC and STA authorize the employee to all **Tenant** Cargo Area/SIDA, AOA and Cargo Area/SIDA of **Airport** when necessary to complete their assigned duties. **Tenant** employees that have been issued an **Airport** ID badge have unescorted access to all areas of the airport. Coordination must be conducted when entering other tenant's leased space.
Tenant employees that have been issued **Airport** ID badge may escort persons in all areas of **Airport**.

The **Tenant** badge is a 3 ½" x 2 ¼" badge consisting of:

- Full face photograph of employee (border color of photo is orange for all **Tenant** employees and white for **Tenant** vendors)
- Full Name, Employee #, Hire Date/Expiration Date
- Company Name
- Barcode
- Ramp Identification – Code for Airport Name
- Unique serial number for each identification badge
- Word "EXCLUSIVE" in red background on left side of badge

Tenant issues ID badges through the Corporate Office at **location** by use of an automated system. Immediate notification must be given to a Manager in the event of a lost or stolen badge. Upon termination all badges must be surrendered to a manager.

Language on ID Media Holder Responsibility

This language is from a tenant security program of a CAT I airport addresses the responsibilities of badged personnel in securing the tenant area.

A. All persons who possess an Airport-issued SIDA Badge or a **Tenant** ID Badge are responsible for ensuring the security integrity of the **Tenant** Operations Area by
   a. Properly displaying their unescorted access authority media (SIDA badge or **Tenant** badge).
   b. Challenging persons without proper ID or those not displaying ID
   c. Reporting suspicious persons, groups or activities to the Police Department the Airport Authority, TSA, or **Tenant** management.

Language on Compliance with ID Media Issuance Requirements

The language below is taken from the ground lease of a CAT I airport, which addresses the need for employees and agents of tenants to undergo security training provided by the airport. The provisions also address the badging requirements for tenant employees, including background investigations.

Lessee further acknowledges that its employees and agents may be required to undergo background checks and take Airport Security and Access Procedures ("S.I.D.A.") training before receiving an Airport Security Identification Badge. Immediately upon the completion of any work requiring airport security access under this lease, or upon the resignation or dismissal of, or conclusion of any work justifying airport security access to, any agent, employee, subcontractor, or invitee of the Lessee, Lessee shall, surrender any Airport Security Identification Badge held by the Lessee or by such agent, employee, subcontractor, or invitee. If Lessee has failed to surrender any such badge to the Authority within five (5) days, the Lessee will be assessed, and pay, a fee for each badge not returned, at the then-current amount set by the Authority for lost badge fees (such fee is currently **$XX.XX** per lost badge).

4.3 Challenging

Challenge requirements are generally seen as an essential part of any tenant security program. Such practices are mandated by airports as part of the airport's security program for regulated areas.[16] The challenge requirements set forth in the regulations serve as the basic model for challenge procedures that appear universally in all regulated and nonregulated tenant security agreements. Although it is typical to follow the federal requirements, in some instances the challenge procedures can go beyond Part 1542 requirements. For example, one airport requires the physical touching and inspection of a badge as part of the challenge. Airports might also consider imposing a record-keeping requirement to better monitor tenant performance of challenge testing.

SAMPLE LANGUAGE

The language below addresses challenge practices and challenge program requirements.

General Language on Challenge Requirements

These challenge provisions come from the EAA template for a CAT X airport. They include instructions for notification in the event a badge is not displayed, as well as provisions that limit the access of other tenants into the area operated under the EAA. However, badged airport personnel are permitted in the tenant area.

> **Tenant** personnel will challenge all persons within **Tenant** Exclusive Security Areas that are not properly displaying a valid **Tenant** or Airport identification badge and will report to the Airport (**XXX-XXX-XXXX** or the **Tenant**/Airport Communications hotline) any person who cannot produce a valid badge and who is not under escort by a properly authorized person. Any person, including **Tenant** employees, found on the secured portion of the airport beyond the **Tenant** Exclusive Security Areas and not in compliance with the Airport Authority's security program will be subject to prosecution for violation of a restricted area. Other **Airport** badged tenant employees, except for Airport employees must obtain permission from **Tenant** before entering the **Tenant** Exclusive Security Areas.

Language on Challenge & Escort Requirements

These provisions from the rules and regulations for a CAT II airport combine discussions of escort and challenge requirements. This rule applies the challenge requirements to both secured and non-secured areas. This is an example of a tenant security provision exceeding Part 1542 requirements. The portion concerning escort in the Secured Area (a & b) is required, but the portion concerning escort in non-secured areas (c & d) exceed Part 1542 requirements.

> **Escort and Challenge Procedures**
>
> a. Individuals authorized unescorted access to the Secured Area may escort individuals who have not been issued media authorizing unescorted access to the Secured Area. "Positive" escort procedures must be used, meaning that the escorted party must be within the sight and hearing of the authorized escort and must be under their control at all times. The escort shall ensure that the escorted party engages only in authorized activities.
> b. In the Secured Area, all holders of airport access media authorizing them access to that area shall verbally challenge any person who is within the secured area without proper access media displayed. Airport Authority law enforcement officers are available for response at any time if needed; telephone, **XXX-XXX-XXXX**.
> c. In the non-Secured Areas, tenants shall be responsible for the security of their leased areas and shall monitor and escort their respective customers to ensure that there is no deviation from authorized areas and activities.

[16] 49 CFR § 1542.211(d)

d. In the non-Secured Areas, it is the responsibility of any holder of airport access media authorizing them access to that area to verbally challenge any person recognized as not having access authorization. Airport Authority law enforcement officers are available for response at any time if needed; telephone, **XXX-XXX-XXXX**.

4.4 Escorting

Given the growing focus on insider threat, there is increasing scrutiny on the escort of people into areas. Like challenge requirements, escort requirements are generally the same as required by those specified in regulation.[17] Those provisions are incorporated into the airport's ASP and should be applied to any regulated areas under tenant control.

The airport should ensure that restrictions are placed on the number of ID media holders with escort authority so that only those individuals with a need to escort are permitted to do so. Those individuals with escort authority need to be trained on their responsibilities as ID media holders with such privileges. While most escort requirements can be communicated through the airport's process for issuing ID media, the incorporation of these types of provisions in tenant agreements seems universally accepted.

If the airport permits tenant issuance of ID media in conjunction with an EAA, it should ensure that the escort provision afforded by the tenant meets the regulatory requirements. In addition, some airports have imposed control measures like visitor logs and visitor badge issuance to help manage escort activity in tenant areas. These measures serve to facilitate airport audits to ensure compliance.

SAMPLE LANGUAGE

The language below addresses escort programs. The escort programs outlined below impose significant obligations, including badging and escort ratios, which exceed Part 1542 requirements.

Language on Escort Requirements for Badged Escortees
This language from a CAT I airport's tenant security plan addresses the issue of escorting in the context of an airport that issues visitor badges to all escortees. It also introduces a 25-foot rule on line of sight that exceeds Part 1542 requirements.

A. Only those persons with RED "Escort" indicated at the top of their Airport-issued SIDA badge may perform escort duties. They shall ensure:
   1. Each person being escorted is displaying an Airport-approved ORANGE Visitor "V" badge.
   2. A 25-foot line-of-sight positive control is maintained and they are in a position to monitor the activities and control the movement of individuals who are under their escort.
   3. A ratio of one (1) escort for every five (5) persons who are in possession of an ORANGE Visitor "V" badge.

Language on Escort Requirements for Non-Badged Escortees
This language from a CAT X airport's EAA template addresses the issue of escorting in the context of an airport that does not issue visitor badges to escorted visitors. It introduces requirements of escort ratio, which exceed Part 1542 requirements.

[17] 49 CFR § 1542.211 (e) and subsequent regulatory enactments

Escort Procedures

The **Tenant** authorizes a limited number of individuals that are allowed to provide escort services within the SIDA/Secured Area. Such individuals must be identified with a proper endorsement on the Airport Security ID card. When it has been deemed necessary for an individual to access the SIDA/Secured Area and the individual has not been issued an Airport Security ID card, and does not possess one of the other accepted forms of ID as listed in the program, the individual must be escorted by an Airport Security ID cardholder with escort privileges.

a. An Airport Security ID cardholder with escort privileges can escort a maximum numberof
   (ii) five (5) individuals and
   (iii) two (2) vehicles at any given time
   Changes to the escort maximum numbers are subject to approval, as stated under Section 4 – Approvals and Amendments
b. Escorted individuals (1 to 5 ratio) must remain under line-of-sight observations at all times while in the SIDA/Secured Area.
c. Escorts must be able to maintain verbal communications with the escorted individuals without the aid of electronic devices such as mobile phones and two-way radios.

In the event an individual under escort engages in activities that warrant the revocation of access privileges, the Airport Security ID cardholder conducting such escort is to immediately revoke access privilege, attempt to escort the individual out of the SIDA/Secured Area, and inform the Airport Duty Manager of the incident. If the situation calls for a law enforcement presence, the call should be made to Police Emergency phone line immediately.

Escorts must be conducted in accordance with the procedures outlined in 49 C.F.R. Part 1542.211.

4.5 Training

Security training is another essential issue for employees and contractors who work in tenant areas and need unescorted access to the SIDA or the AOA. Airports need to ensure individuals accessing these areas receive training in accordance with the regulations.[18] This is a requirement addressed in most agreements, and is mandatory for EAAs and ATSPs.

While training is usually offered in connection with the airport's credentialing process, airports can—and in some tenant agreements do—place the burden of that training on the tenant. Ensuring training occurs is a particular concern in an EAA, which allows a tenant to issue ID media. However an airport determines is best to handle this issue, the training offered to individuals with unescorted access must follow TSA-approved curriculum. The method of delivery must also be approved by the TSA.

SAMPLE LANGUAGE

The language below addresses training programs. Specifying training and the entity responsible for administering that training are important issues. While it is often done in connection with credentialing, it becomes particularly important for an EAA where the tenant issues ID media.

Language on Escort Requirements for Training (Tenant Responsibility)
This language from a CAT X airport EAA outlines security training requirements for employees or contractors of the tenant operating the EAA. This language could be adapted for non-EAA airport agreements where the training responsibilities are passed to the tenant.

[18] 49 CFR 1542.213 (b) and/or (c)

Tenant must train the relevant contract personnel on their specific security responsibilities and the procedures required by this Agreement. Such training shall occur quarterly. All Tenant employees must receive site specific SIDA and security training during onboarding process and every time there is a change to the Security Handbook or change to this EAA. Upon request by Airport or the TSA, Tenant will immediately provide documentation to establish that such training has occurred.

Language on Escort Requirements for Training (Airport Conducted Responsibility)
In airports where the training is conducted by the airport, the language offered by this CAT II airport EAA may be more helpful.

Each Tenant employee is actively involved in preventing the unauthorized entry of persons into the Airport SIDA and or AOA. Prior to issuance of an Airport Badge/Tenant Issued media, each employee is trained in airport security rules and regulations through Airport Security Awareness Training as instructed through the Airport ASP. In addition, yearly Tenant employees with Airport AOA / SIDA badges are required to renew their training through the Airport Security Awareness training program offered by Airport Security and they are to acknowledge the provisions of this EAA. Said training is required upon initial hire through Airport Security and again annually every year as outlined above.

4.6 Inspection

Provisions for inspection vary greatly among airports. Some have fixed inspection schedules, while others have more informal practices. Types of inspections can include reviews of documents, such as access control records, in addition to physical inspections of the tenant facility areas.

Inspections of EAAs are generally only conducted by TSA. Airports can, however, reserve the right of inspection in any agreements that they execute. That right of inspection is particularly important in circumstances where the primary responsibility for inspections does not rest with the TSA. All agreements should indicate that the TSA has the right to conduct inspection of tenant areas in addition to any inspection the airport may or may not conduct.

SAMPLE LANGUAGE

The language below addresses the right to inspect of tenant areas. This should include inspection by both the airport and TSA, and may include property and records inspections. In drafting inspection language, the airport may want to consider measures to require remediation of deficiencies.

General Language on Compliance Inspections
This inspection provision comes from the EAA template for a CAT X airport. It affords the airport and the TSA the right to inspect.

Right of Inspection

Tenant understands its obligation and will allow the Airport or its authorized representative and the TSA, pursuant to CFR 1542.5, access to all areas outlined in this plan for the purpose of compliance inspections. These inspections may occur at any time and without prior notice to Tenant.

Inspection can also extend to the records of a tenant. This language from a CAT X EAA template outlines the authority of the airport to inspect records and documents relevant to tenant badging operations.

Employee CHRC, training and related ID information will be available for inspection by **Airport** and TSA. All information will be retained for a period of **XXX** days after employment has ended.

Language on Inspection and Remediation
This inspection provision comes from the EAA template for a CAT X airport. It affords the airport and the TSA the right to inspect and require remediation of deficiencies.

Right of Inspection & Amendment

The **Airport** shall have the right to inspect the Exclusive Area to ensure compliance with this agreement The Tenant will correct any problems noted by the **Airport** immediately by initiating corrective action. This does not obligate the **Airport** to conduct such inspections or to be responsible for identifying or correcting such problems.

If security requirement (federal, state, or airport) conditions change, the **Airport** shall have the right to review and amend this agreement.

4.7 Audit

ATSPs require audits because the airport is in a position to oversee tenant security operations; airports do not commonly include audit provisions in other types of tenant facility agreements. With respect to EAAs, there is no audit function mandated, and most airports with EAAs do not audit tenant security operations.

Most audits that are conducted by airports under ATSPs are limited to credentialing, visitor logs or tenant access control records, key control, or annual reviews of the tenant arrangements. Most of those audits are performed on an annual or semi-annual basis. Even if an airport chooses not to impose a schedule of audits on its tenants, reserving the right to audit is something an airport may wish to consider in preparing its agreements.

Audits may be required by an airport in other types of security agreements. Where an airport decides to conduct audits, it should consider including a general assessment of physical security measures and security practices to ensure compliance with the measures and practices specifically delineated in the security agreement. Not infrequently, tenants will make changes in the physical layout of a facility or alter operational practice, which necessitate changes in security arrangements. If those changes are properly documented, and the airport is notified and grants permission for them, the alterations do not pose a significant difficulty. If, however, changes are made without notice and authorization, they can create security risks. Regular audits to compare actual measures and practices with those provided for in the security agreement can help mitigate those risks.

SAMPLE LANGUAGE

The language below addresses the right to audit tenant operations. The research found that common subjects of security compliance audits include key control records, visitor logs and records, ID media issuance records, and access control. These audit provisions specified issues like audit frequency and penalties for failure to comply.

Language on Compliance Audits for Access Control
This provision from the tenant security agreement of a CAT I airport offers an example of audit requirements for access media and key control.

The Authority shall monitor and audit the **Tenant** for compliance of all airport issued Identification Media (ID) and lock and key requirements.

(1) Quarterly and Annual Audit Reports

(a) Quarterly, the **Tenant's** Authorized Signer shall forward a spreadsheet audit of all active security badged employees to the Airport Authority badging office. Minimum information forward shall be current badge employees full name, badge type, badge number and expiration date.

Failure to forward the report within 30 Calendar Days of the due month may result in the deletion of access media authority for all employees of that company, and any attempt to use the access media will be recorded as an invalid attempt to gain entry and access will be denied.

(b) Annually or as requested, Lock and Key (including number type code pads) audit information shall be forwarded to the Airport Security Badging office. The **Tenant** shall maintain, monitor and control all access to the AOA/SIDA from their facility or leased area. **Tenant** shall practice strict lock and key control issuance procedures and shall be required to secure un-issued keys and maintain records to document the tracking of all issued keys. Cipher code access (number code pads) shall have the code change annually. All keys that would allow access to the restricted area shall be marked "Do Not Duplicate" or "Restricted" and serial numbered.

Language on Compliance Audits for Visitor Access

This provision from the tenant security program at a CAT X airport addresses audit requirements around visitor access at the tenant facility.

At a minimum annually, the airport will perform an audit of the visitor logs, and the facility in order to assure that these established procedures are still followed. The results of the audit will be kept by the Airport Security Coordinator. **Tenant** will keep internal visitor logs for a minimum of **XX** months for audit purposes.

Language on Compliance Audits for ID Media

The provisions of this tenant security program utilized at a CAT X airport address the airport's right to audit records relating to tenant badging operations.

An annual audit will be jointly performed by **Airport** and **Tenant** Security representative to identify all current and past employees and others that have been issued a **Tenant** ID badge at **Airport** and **Tenant** Security personnel (that have been granted unescorted access to **Airport**). The audit will also include a review of current **Tenant** Stop List. After each audit an updated list and the result of the audit will be signed by the Sr. Manager of the **Tenant** location or his/her representative and provided to **Airport**. **Airport** badging office will maintain a copy of this audit for a period of one year and reserve the right to require additional information.

4.8 Security Personnel

Deployment of security personnel is not typically addressed in most formal or informal arrangements. Some templates for EAAs and ATSPs contain language that addresses requirements, such as establishing post and setting staffing levels. Most often those matters were left to the discretion of tenants in other types of agreements.

SAMPLE LANGUAGE

The language below addresses tenant security staffing issues, including posts and schedules.

Specific Language on Security Staffing

This matrix from a CAT X airport's EAA outlines specific staffing requirements for areas in the EAA. The provision on staffing requirements outlines general staff and supervisory levels, and requires

completion of the matrix to outline staff deployments. This matrix can be adapted for non-EAA airport agreements where the staffing responsibilities are passed to the tenant.

BUILDING X – AIRLINE/AIRPORT TENANT GUARD SERVICES				
Guard Post/ Position	Guard Location	Area(s) Covered	Hours of Operation	Duties/Description

General Language on Security Staffing
This language from a CAT X airport's EAA outlines more general staffing requirements for access points. This language can be adapted for non-EAA airport agreements where the staffing responsibilities are passed to the tenant.

1. **Tenant** will accomplish access control at each access point to the **Tenant** Exclusive Security Areas by:
   a. Maintaining properly staffed security posts or computer-assisted access control points or both at each **Tenant** vehicle and pedestrian gate used to enter the **Tenant** Security Areas. **Tenant** will review security post orders semi-annually and will make those orders available for inspection with the Airport or TSA security inspectors.

4.9 Security Practices

Generally, specifics on security practices are only included in tenant facility agreements that specify patrol routes or frequencies, posts or post orders, or other security policies. Some airports may choose to address these issues through EAAs, ATSPs or other security agreements Similarly, training requirements for security personnel are not specified, though this may be because training is required for the issuance of airport ID media. However, in some larger airports, specific training curricula and requirements for both tenants and even the third-party security personnel employed by tenants was specified. As with the detailing of specific security practices, the requirement for specific security training gives the airport greater control over the quality of tenant security, but it may have cost and contract management factors that should be considered.

SAMPLE LANGUAGE

The language below addresses tenant security plans and practices. This includes issues such as staff deployments, patrol activities, and response requirements. Annual submission of tenant security plans is a method of ensuring continuous review of tenant security requirements.

Specific Language on Tenant Security Plans/Practices
This language from a CAT II airport Minimum Standards document requires tenants to develop their own security plans and submit them to the airport for approval. Those plans are required to be integrated with regulatorily mandated security requirements.

Operator shall develop and maintain a Security Plan.
Security Plan shall be submitted to the Commission for review and approval no later than 30 calendar days before Operator is scheduled to commence Activities at the Airport.

The Security Plan shall be resubmitted any time changes are made clearly showing all changes against the prior version of the Security Plan. The Commission shall have 30 calendar days to review the amended Security Plan before the amended Security Plan becomes effective. During such 30-

calendar-day period, the Commission may require Operator to implement reasonable modifications to the Security Plan, which Operator shall be required to implement. Thereafter, Operator shall re-submit such amended Security Plan with the Commission's required modification. The Commission shall have **XX** calendar days from such resubmission to review and approve the amended Security Plan.

Upon request, Operators that are required to comply with a TSA security program must demonstrate compliance to the Commission's satisfaction with all applicable TSA requirements to the Commission within **XX** calendar days.

Operator must comply with applicable reporting requirements as established by the Commission, FAA, DHS, TSA, and any other Agencies.

Specific Language on Tenant Patrol/Response Activity

This language from a CAT X airport's tenant security program outlines requirements for coordinating security patrol activities, and indicates the presence of police and security patrols provided by the airport.

Security and Law Enforcement Patrols

- Security and Law Enforcement patrols are conducted by **XXX** Police and provide surveillance, act as a deterrent, and respond to security-related incidents. Both **XXX** Police and Airport Authority Personnel provide 24/7 security and law enforcement patrols at **Airport**. When the security level increases at **Airport**, additional patrols are conducted.
- Other patrol activities will be determined by a collaborative effort in conjunction with **XXX** Police and Airport Authority Personnel as deemed appropriate.

4.10 Changed Conditions

All agreements should consider reporting of changed conditions affecting security as a baseline requirement. It is a clear requirement of EAAs and ATSPs, and it is present in most tenant security programs. It is also found in tenant provisions in some airport rules and regulations.

The inclusion of changed condition notification and response requirements is essential to maintaining continuity in an airport's security posture. Tenants need to understand that if a security measure fails or malfunctions, the airport and TSA need to be advised, and satisfactory alternative measures must be employed to maintain security until the original measures can be restored. If the tenant is incapable or unwilling to implement alternate measures to ensure the continued security of the facility, the airport will be expected to do so. This issue should be addressed in agreements with the tenant. Such provisions might be included in the EAA, ATSP, other tenant security program or underlying lease agreement. The airport may also wish to include express provisions for the possibility of the assignment of cost in the event the airport is required to address security issues on the tenant's behalf.

Provisions on changed conditions should apply to both unexpected and planned changes. This raises the important issue of addressing tenant improvements. To help prevent tenants from inadvertently implicating changed security condition requirements without proper TSA and airport approvals, airports should contemplate adopting some form of program for review and authorization of tenant improvements. This program should include a security review of any construction, to include temporary measures during construction, that ensures proper security arrangements are put in place, and any necessary notices and approvals from TSA are secured. Some airports include tenant improvement processes in their regulations.

SAMPLE LANGUAGE

Notice of changed conditions is a regulatory requirement for EAAs and for ATSPs, and is advisable for any tenant security arrangement. Language should address both planned and unplanned changes. Frequently, changed conditions issues arise in connection with tenant improvements, warranting special attention to managing tenant improvements. Airports may also want to consider adding language that outlines the need for tenants to add security measures in response to changed security conditions, and to permit airports to remediate conditions if the tenants are unwilling or unable to do so.

General Notice of Changed Condition

These general notification provisions concerning inability to maintain security requirements come from the EAA template for a CAT X airport.

If **Tenant** is unable to comply with this Agreement or when the procedures described in this Agreement are not adequate to perform the control functions described, **Tenant** security personnel will promptly notify in writing the Airport Authority's security coordinator.

Specific Language Addressing Planned and Unplanned Changes

The following language from a CAT X EAA template addresses both planned and unplanned changes, and provides greater specificity than the requirements in Part 1542.11. In addition to use in EAAs or ATSPs, language concerning changed conditions reporting is commonplace in other tenant security arrangements.

Tenant must immediately notify the TSA and the Airport representative (the ASC/ASM, or his/her designee) when changes have occurred to the area descriptions, or other measures or other measures described in this EAA.

A. Planned changes

When there is a project that will involve a change in any of the security features of the facility (i.e. construction that involves access control doors, etc.), **Tenant** must notify the Airport representative (the ASC/ASM or his/her designee) and the TSA, and begin the security amendment process at least **XX** days or at the earliest reasonable time prior to any planned changed condition under 49 C.F.R. Part 1542.105(b) (amendment to the security program). The amendment request must be reviewed and approved in writing by the TSA and the Airport prior to any changes being made. In addition, **Tenant** must submit a Tenant Alteration Application (TAA) to Airport's designated representative if applicable.

B. Unplanned changes

Tenant must notify the Airport representative (the ASC/ASM, or his/her designee, or if not available, the Airport police department or the designated Airport representative (if the Airport police department is not available) by phone and with a follow-up email no later than **XX** hours after the discovery of any changed condition, so the Airport can inform the TSA within the timelines prescribed by TSA regulations. **Tenant** must inform the TSA and the Airport of each interim measure being taken to maintain adequate security until an appropriate amendment to the security program is approved. Each interim measure must be acceptable to the TSA and the Airport.

Language Addressing Planned Changes Through Permitting

One CAT X airport approaches the problem of managing tenant improvement through the establishment of a permitting process for tenant improvement.

Work at the Airport. No other Person shall perform any alterations, improvements, repairs, construction, or other similarly related work (i) within the terminal buildings and the Restricted Areas, or (ii) on other Airport property that is not under lease with the Board, without first obtaining a permit issued by the Airport's Planning and Development Department. The permit shall be on display continuously for the duration of the work at the

Airport. The form of the application and permit shall be as prescribed by the Airport's Planning and Development Department. The permitting process is for the Airport's internal purposes only and does not relieve any Person from compliance with all other applicable laws related to the work. The permitting process shall not be construed to be approval for architectural or engineering design or compliance with applicable laws or codes. on 01.02(9) shall not apply to employees of the Board or Persons under contract with the Board to perform work.

Language Addressing Planned Changes Through Tenant Improvement Review Process

This language from the rules and regulations of a CAT I airport outlines the general responsibilities of tenants to participate in an established process for alterations and improvements on their leased premises. These changes can involve or alter established security infrastructure (e.g., requiring the closure of access-controlled doors or movement of fencing), requiring the preparation of changed condition amendments.

Construction or Alteration of Improvements

Prior notification must be given to Airport management before commencing any construction or alteration of an Improvement and shall be performed in compliance with the Airport's Tenant Improvement Process and Standard Requirements described in Appendix 12.10 and the Airport's Tenant Remodeling Electrical Specification Requirements identified in Appendix 12.7.

Tenant Improvement Process and Standard Requirements

Purpose: The following describes the standard operating procedure and process for review and approval of all tenant improvements at the Airport. The provisions insure and promote overall safety, security, comfort, convenience and efficiency for all customers using Airport facilities. The provisions also promote a smooth construction process that minimizes disruption to our customers, and to the operations of other Airport tenants and the County.

Enforcement: Adherence to this process is required as part of the Agreement between the County and the tenant, and shall apply to sub-tenants through extension. Enforcement of the provisions contained in this process shall primarily be the responsibility of the County. The TSA, FAA, Occupational Safety and Health Administration (OSHA), and the Sheriff's Department also have the authority to enforce laws, federal regulations and the Airport Security Program. Failure to comply with the provisions, procedures and standards contained in this document may result in the delay, postponement or cancellation of the proposed improvement. Additional sanctions may be imposed on the tenant by County as are deemed necessary.

Language Addressing Response to Changed Requirements and Airport Right to Remediate

The following provisions taken from the tenant security program of a CAT I airport recognize that security requirements may change, necessitating tenant compliance with the changed requirements. The provision requires tenant compliance at its expense, and permits the airport to make necessary improvements and bill the tenant.

The Authority's Executive Director, or his designated representative, may, from time to time, evaluate **Tenant's** compliance with the security procedures set forth herein, as such procedures may be amended. TSA may issue Security Directives or raise the threat level that results in a change in security conditions that the company is required to meet. Such change in conditions will be communicated by the Director of Public Safety and must be implemented as instructed. Failure by **Tenant** to fully implement and comply with such procedures will be sufficient cause for the Authority to take any immediate corrective measures deemed necessary, in the Authority's sole judgment, including closing access from the Premises to the AOA until acceptable security is restored by **Tenant**. In the event that **Tenant** is temporarily unable to perform its authority and responsibility hereunder or is otherwise unable to comply with provisions of this Agreement, **Tenant** shall immediately notify the Authority's Executive Director, or his designated representative, who shall immediately take whatever corrective action is deemed necessary, in the Authority's sole determination, to reestablish and maintain the

required level of security. All costs incurred by the Authority for any such corrective activity by the Authority hereunder shall be paid by **Tenant** upon receipt of an invoice therefor from the Authority.

4.11 Notice of Events or Incidents

Provisions concerning required notice of security-related incidents and events vary greatly among agreements. A baseline notice must be provided for changed conditions affecting security, but some notice provisions also include requirements for reporting other incidents or events affecting security operations. Airports operating 24-hour aviation operations centers or security operations centers are more likely to have expanded reporting requirements for incidents or events.

SAMPLE LANGUAGE

Airport security managers frequently voiced concern over notification of incidents and entrusting the security authority to tenants. Those concerns included timeliness of notifications, failure of tenants to self-report tenant security incidents, and failure to provide adequate actionable information. The language below offers a range of approaches to the issue. Use of this language does require that the airport have mechanisms in place to receive and process this data—for example, an operations center or other centralized call center to receive, process, and initiate action in response to the information. Agreements vary in the level of specificity required, both with respect to the filing of reports and the amount of information required.

General Notice of Security Incidents or Issues

These general notification provisions concerning security incidents come from the EAA template for a CAT X airport.

1. **Tenant** security personnel will immediately notify the Airport's Security Coordinator (ASC) or his/her designated representative each time **Tenant** personnel have an unresolved question concerning airport security.
2. **Tenant** personnel will immediately notify the Airport Police Department (LEO) (24/7 number **XXX-XXX-XXXX**) of any suspicious activity (persons or vehicles).

Detailed Reporting Requirements

This language, which is from the tenant security program of a CAT II airport, imposes more detailed reporting responsibilities, and includes detailed information on the actions to be taken.

The Tenant Access Control Contact (TACC) will make immediate notification to the Airport Security Coordinator of any instance of non-compliance with this Tenant Access Control Program.

The Tenant Access Control Contact or his/her designee, when notified or becomes aware of an incident or suspicious activity or threat information that could affect the security of Airport or US Civil Aviation must notify Airport Operations as soon as practical. Incidents, suspicious activities, and threat information may include, but are not limited to incidents of interference with flight crew, specific or non-specific bomb threats, any information relating to the possible surveillance of an aircraft or airport facility that could indicate a potential threat to civil aviation.

The following information, as it is available and to the extent not legally prohibited, shall include in this report:

1. The name of the reporting individual and call back number
2. A description of the threat/incident/suspicious activity.
3. The names and other biographical data, as available, of individuals involved in the threat, incident, or activity.
4. The source of any threat information.

This language from a CAT X airport's proposed ATSP template addresses notice of incidents and events that may affect an airport's security. It includes detailed information on both the type of incidents to be reported and the actions to be taken.

1. **Tenant** must immediately notify the Airport Operator of any incident, threat information or suspicious activity that may compromise the integrity of the security responsibilities as outlined in this ATSP. In addition, a sweep of the affected area must be conducted for resolution.
   a. Security-related incidents, threat information, and suspicious activity include, but are not limited to the following:
      i. Specific or nonspecific bomb threats
      ii. Unauthorized surveillance of the facility
      iii. Any security-related incident that results in a law enforcement officer (LEO) or first responder being dispatched to the facility
      iv. Any unauthorized individual discovered within the facility who's location cannot be confirmed
      v. Any individual on the Airport Operator stop list that attempts to gain access
   b. Security-Related Incidents will be reported to the Airport Operator Operations Office at **(XXX) XXX-XXXX**
   c. The report must include the following information:
      i. The name and contact information of the individual reporting the incident
      ii. The time and date of the incident
      iii. A description of the incident, suspicious activity, or threat
      iv. Any follow-up information if required

4.12 Sanctions

Every airport has different penalties for failure to comply with security requirements. These penalties may include retraining of individuals or fines against the individual or company. Regardless of the type of consequence or the agreement type, the penalties should be clearly defined within the agreement. This should also include potential consequences that may be levied by the TSA.

Addressing tenant failure to comply with security requirements is commonplace across the differing arrangements for tenant facilities. Airports use several mechanisms to address those issues:

4.12.1 Indemnity/Hold Harmless

Indemnity provisions can be found in leases, security agreements, and rules and regulations. They generally cover, at a minimum, costs associated with fines and penalties in connection with TSA actions. The scope of the indemnity can vary and, in some cases, it is expanded to include issues such as attorneys' fees and costs in connection with defending against TSA actions.

SAMPLE LANGUAGE

The language offered below provides an example of a broad-based indemnity/hold harmless provision and one more narrowly crafted to address fines imposed by the federal government.

Broad Indemnity/Hold Harmless Language
This is a hold harmless and indemnity provision from the Minimum Standards document of a CAT III airport.

Hold Harmless

Each Agreement with an FBO or SASO, or any other Entity doing business on the Airport, shall indemnify and save the Authority, its officers, and employees harmless from and against any and all claims, suits, actions, damages, and causes of action, arising during the term of any bodily injury, loss of life or damage to property sustained in, about, or upon the Leased Premises occupied or used by any such Entity, FBO or SASO, or the buildings and improvements placed thereon, the appurtenances thereto, or any other claims or suits arising out of the Agreement, and shall indemnify and save the Authority harmless from and against all costs, counsel fees, expenses, and liabilities incurred in or about any such claim, the investigation thereof or the defense of any action or proceeding brought thereon and from and against any orders, judgments or decrees which may be entered therein. Each Agreement further shall provide that any such Entity, FBO, or SASO shall defend any action, complaint, or proceeding brought against the Authority as the result of any of the matters above delineated, all at no cost or expense to the Authority.

Indemnity/Hold Harmless for Fines and Penalties

This language from the ground lease of a CAT I airport specifically addresses the issue of indemnification for security-based fines, though it appears to predate the creation of TSA.

Lessee acknowledges that the Authority is subject to strict federal security regulations limiting access to secure areas of the airport and prohibiting violations of the adopted Airport Security Program. Lessee may need access to these secure areas to complete the work required by this lease. Lessee therefore agrees, in addition to the other indemnification and assumption of liability provisions set out above, to indemnify and hold harmless the Authority and **XXX** County, and their respective commissioners, officers and employees, from any duty to pay any fine or assessment or to satisfy any punitive measure imposed on the Authority or **XXX** County, by the FAA or any other governmental agency for breaches of security rules and regulations by Lessee, its agents, employees, subcontractors, or invitees.

4.12.2 Liquidated Damages

These types of provisions are contract remedies, generally used only in connection with leases or other agreements. They provide estimates for damages that are difficult to quantify and calculate, for example impairment of airport brand or some categories of business or operational loss.

SAMPLE LANGUAGE

The language offered below provides an examples of liquidated damage provisions.

Lease-Based Liquidated Damages

One CAT I airport includes a liquidated damages type penalties provision in its lease agreement. This allows the authority to assess penalties from a set penalty schedule for a range of operational violations, including security violations.

The failure of Concessionaire to adhere to the requirments outlined in the Lease will result in inconvenience to the public and adversely affect the operation of the Airport. Quantification of the resulting damage is difficult. Concessionaire agrees to pay to Authority penalties in accordance with this Article, at the rates or in the amounts specified below, upon the occurrence of the specified breach and upon written demand by Authority

Except for Lease violations regarding the minimum hours of operation, fire, life, health, or safety issues and pricing violations, the penalties for which shall be incurred immediately, the penalties for the first violation of other standards may only be imposed when the violation continues for more than three (3) calendar days after Authority has given Concessionaire notice of the violation, provided, however, after Authority has given Concessionaire notice of the same violation more than twice during any Lease Year, the penalty shall be immediately imposed.

The penalties provided for in this article are intended to mitigate the damages resulting from the inconvenience ot the public and the adverse effects on Airport operations; payment of penalties are in addition to any other remedies Authority have under this Lease or applicable law and shall not relieve Concessionaire of any other responsibility it may have including responsibility for personal injury. Or other harm caused by Concessionaire, or its employees, agents or tenants.

For non-monetary defaults under this Lease, Authority in its sole reasonable discretion may determine if a violation of this Lease has occurred and may impose the penalties pursuant to this Article. Authority shall provide written notice of each offense to Concessionaire. Failure to pay the penalty wihtin thirty (30) days of such notice shall constitute a default under this Lease. Violations in this Article are cumulative during each Lease Year.

Concessionare agrees that such penalty amounts are fair compensation to Authority for the damages caused by the violation.

For those violations where a plan is required to correct the violation, then Concessionaire shall develop such a plan, including a time schedule under which resolution can be achieved for Authority's review and approval.

Lease-Based Liquidated Damages

The following liquidated damages provision is taken from the tenant security program of a CAT I airport.

In the event any personnel of **Tenant**, or its contractors, are judged by the Authority or Transportation Security Administration (TSA), in their sole determination, to have committed a Security Violation, Company hereby agrees to pay the Authority, as liquidated damages and not as a penalty, **$XX.XX** for each such Security Violation not classified as an airfield incursion. (As used herein, a "Security Violation" shall mean the unauthorized admittance to the restricted area of the Airport and/or the Premises within such secured or restricted area of any vehicle without the proper permit or any personnel that have not received proper identification media.) Such sums shall be in addition to any civil fines or penalties from TSA or any other governmental agency which may be assessed against the Authority or Company as a result of such Security Violation(s), which fines or penalties Company also agrees to pay to the Authority, TSA, or other governmental agency. Civil penalties are currently in an amount up to **$XX.XX** and may be changed from time to time.

4.12.3 Fines and Penalties

Fines and penalties can be imposed by the TSA for violation of federal regulations. Unless the entity is regulated, such as an airport or air carrier, those fines and penalties are generally targeted at individuals covered under the scope of the regulations.

Airports can also impose fines and penalties in the exercise of governmental functions. This is generally done in conjunction with rules and regulations, or ordinances published for operation at the airport. The ability to set fines and penalties depends on the governmental structure of the airport; some require permission from other entities, like city councils or county boards, to enact or modify fine or penalty provisions.

SAMPLE LANGUAGE

The language below provides an example of regulatory fines and penalty provisions. These types of provisions generally reference a schedule of fines and penalties that lays out penalty amounts for certain infractions. The provisions address issues like notice, and may also afford airports the ability to directly mitigate certain conditions (usually those that pose health or safety risks).

Local Regulatory Fines and Penalties Provision
This language, taken from the operating regulations of a CAT X airport, provides a comprehensive approach to addressing compliance with the assessment of fines along with self-help provisions. This allows the airport to remediate dangerous conditions at the cost and expense of the tenant.

Types of Violations, Penalties and/or Administrative Assessments

The Director is as authorized and empowered by the Board of County Commissioners to issue written Operating Directives in order to implement the provision of Title 20 and Airport Rules and Regulations and to ensure compliance with all federal, state, and local laws, ordinances and regulations. As such the Director of Aviation is authorized and empowered to issue contractual penalties and/or administrative assessments upon any commercial lessee, permittee, or other commercial user of the Airport, at the Director's discretion, up to **$XX.XX** per violation, per day, for any violation to the Airport Rules and Regulations and/or Operating Directives, and/or terms of any commercial lease agreement, or permit which regulates the conduct of operations at the Airport. Said contractual penalty and/or administrative assessment is in addition to the remedies permitted in any lease, agreement, or permit. Each day (24-hour period) shall be considered a new violation. Certain excessive violations, such as accidents, drug/controlled substance use, or security violations, may require a maximum penalty and/or assessment action to be taken immediately.

Any such contractual penalty and/or administrative assessment shall not exclude or be intended to infer that such contractual penalty or administrative assessment would replace or is instead of any other fine, assessment, or other similar penalty that may be issued by an appropriate regulating agency. If a second Notice of Violation is required, a monetary fine and/or administrative assessment, or other similar penalty that may be issued by an appropriate regulating agency.

Notice of Violation:
In the event that either tenants or contractors fail to comply with applicable federal, state, local and/or Department of Aviation (DOA) safety and health standards, regulations, or operating directives, the Director or designee, has the enforcement authority to enforce compliance with all applicable standards, regulations, or operating directives. For each violation found, a Notice of Violation will be forwarded to the appropriate party (violator).

The first Notice of Violation will be in writing and a written response will be required within ten (10) days of issuance, once the violation has been abated or if the Notice of Violation is being contested.

If a second Notice of Violation is required, a monetary fine and/or administrative assessment may be included. Again, a written response, within ten (10) days of issuance will be required once the violation is abated or if the Notice of Violation is being contested.

If a violation has created a situation considered an Imminent Danger, serious and/or a Willful Offense, the Director or designee has the authority to issue stop work orders, without penalty to contracts or agreements, and the Director or designee can proceed with the abatement of the violation with the responsible party being responsible for all reasonable costs incurred for the abatement of such violation(s).

4.12.4 Suspension and Revocation

Violations of security provisions can result in suspension of privileges by the TSA. Similarly, suspension or revocation of privileges is a possibility provided for in many lease agreements. Where a tenant is not in compliance with lease terms, the lease may be terminated and the tenant removed. Such actions will likely require some legal process to exercise, which may involve administrative or court proceedings or both. Airport regulations and operating agreements can also provide for suspension or revocation of operating privileges. In many cases, the use of badging regulations to suspend privileges of individuals can also be employed.

SAMPLE LANGUAGE

The language offered below provides an example of a revocation penalty. These are common with respect to the revocation of unescorted access privileges, but may also be applied to other tenant privileges.

Revocation of Unescorted Access Privileges

This regulation from a CAT X airport's operating directives provides for revocation of unescorted access privileges, as well as indemnification in the event of TSA-imposed fines and penalties.

> In the event that a tenant, its employees, invitees, officers, agents, representatives, contractors, subcontractors, suppliers, and/or sublessees cause any security violation, and should the Department of Aviation be cited for a civil penalty for such security violation, the tenant agrees to reimburse the Department of Aviation for any monetary civil penalty, which may be imposed by the Transportation Security Administration (TSA). The tenant will have badge/access privileges immediately suspended and/or revoked by the Airport Security Manager for failure to adhere to the Airport Security Program or for failure to return all badges within the time frames specified herein. Such actions may also result in the immediate termination of any applicable operating permit or lease agreement, at the sole discretion of the Director.

4.12.5 Hearing/Review and Appeals Processes

The rules and regulations that enable the airport to impose fines and penalties also provide for administrative review or appeal of those sanctions. These appeals processes are creations of state law or local ordinance and vary significantly from jurisdiction to jurisdiction. Typically, rules and regulations offer some hearing process before an appointed hearing or review officer. Whatever the hearing, review, and appeals process is for fines or penalties imposed, it should be referenced or outlined in the agreement.

Note that review provisions for sanctions resulting from rule violations are separate from provisions associated with lease agreements. The process for imposing penalties under a lease agreement and any associated review would be addressed by the specific terms of the lease.

SAMPLE LANGUAGE

The language offered below provides an example of an appeal/review procedure. The right of appeal is often governed by airport regulation.

Appeal/Review Process

This language, from a CAT X airport's operating regulations, lays out a process for tenants to appeal decisions made on fines or penalties.

> **Appeals Process:** The Director of Aviation or designee will consider appeals on a case by case basis and will respond in writing within fifteen (15) working days after receiving a written appeal.
>
> 1 **Time Limit:** The tenant may appeal a NOV, Airfield Citation, or Parking Infraction, in writing, within fifteen (15) working days of the date of the written notification from the Director of Aviation.
> 2 **Letter of Appeal:** The tenant shall send a letter of appeal to the Director of Aviation. The letter shall include the following information:
> a. A copy of the NOV or Airfield Citation.
> b. A copy of any previous written correspondence.
> c. Documentation of corrective measures thus far implemented.
> d. Remedial action measures that will help ensure that the violation is not repeated.

3 Tenants may further appeal the decision of the Director of Aviation to the Board of County Commission, in writing, within ten (10) working days after receiving the final written decision from the Director of Aviation. Any such appeals shall include the information required above and a copy of the final written decision from the Director of Aviation.

SECTION 5: INFRASTRUCTURE AND EQUIPMENT TO SUPPORT TENANT SECURITY PROGRAMS

Common security infrastructure includes physical ACS (automated and non-automated), signage, lighting, fencing, and sensor surveillance systems like CCTV. Airports have deployed a number of approaches to address infrastructure and technology in support of their security arrangements.

After the discussion in each section below, examples of language addressing those concerns are provided. The excerpts of language appear in gray boxes with any changes from the original appearing in **blue**. The language is taken directly from a variety of sources, including EAAs, ATSPs, other tenant agreements, leases, and rules and regulations from airports of varying sizes. The type of arrangement the language was taken from and size of the airport is noted for each excerpt.

The sample language is not meant to be comprehensive for every scenario an airport may encounter. Airports looking at this language are encouraged to adapt these samples to their own needs and requirements.

Airports using the sample language in their own agreements should consult their airport legal department to review the document.

5.1 Access Control Infrastructure

Infrastructure to support access control is a key part of all airport security plans, including tenant security plans. The types of infrastructure used vary greatly between airports, and even within a single airport. Automated ACS, lock and key systems, and cipher locks are critical parts of the security infrastructure in all airports. Some airports approach these issues generally, but others provide greater specificity with respect to the infrastructure supporting access control.

SAMPLE LANGUAGE

The language below includes example provisions delineating airport and tenant responsibility for security and access control infrastructure.

General Responsibility for Security Infrastructure
This language from the rules and regulations of a CAT II airport outlines the general responsibilities of tenants in maintaining security infrastructure, to include fencing, gates, doors, lighting, and locks.

> Fencing, doors, gates, lighting, and locks which are part of the Leased Premises or have been installed by the **Tenant** must be maintained by the **Tenant** and kept in working conditions at all times. Perimeter fencing and associated doors, gates, lighting, and locks will be maintained by the **Airport**.

Responsibility for Access Control Infrastructure
This language from the rules and regulations of a CAT I airport outlines the general responsibilities of tenants in maintaining ACS. Greater detail is found in the facility access plan executed by each tenant.

> **Operator, Lessee, and Sublessee Rules and Regulations**
>
> **Security**
> All gates, chains, doors, fences, lighting, locks, and all other safeguards that are part of the Leased Premises or have been installed by the Operator must be continually and conscientiously maintained by the Operator and kept in “like new” working conditions at all times. Gates or doors that provide access to the AOA or

Restricted Area through the Leased Premises shall remain closed, locked, properly monitored, and secured except when actually in use. Perimeter fencing and associated doors, gates, lighting, and locks will be maintained by Airport management.

Active logs of keys, access cards, and other media issued (and to whom issued) that allow access to the Leased Premises must be maintained. The log shall be made available to Airport management upon request. Any lost or stolen keys, access cards, or other media shall be immediately reported to the Airport Operations Control Center or Airport ID Badging Office. All applicable reporting requirements must be fully complied with as established by Airport management, FAA, Department of Homeland Security (DHS), Transportation Security Administration (TSA), and any other Agency having jurisdiction. Objects that could facilitate unauthorized access to a Restricted Area shall not be located within six (6) feet on either side of the Airport perimeter fence or any other distance that may facilitate unauthorized access.

Responsibility for Access Control Infrastructure

This language from a CAT I airport addresses the issue of buildings with automated ACS common to the airport as well as key-controlled portals.

Tenant Buildings

The only tenant buildings that provide access to the Secured Area is the **Tenant** facility, and the access points are listed in Section 3.3. 3. The **Tenant** access points are either on the **Airport**-controlled Automated Access Control System (AACS) or have tenant-controlled lock and key controls that prevent unauthorized access. The lock/key system is controllable, auditable, by **Tenant**, and subject to the same procedures as **Airport** controlled lock and key procedures described in Section 4.3.4. The accountability of keyed access to locks on access points to the Secured Area must always be 100 percent or the locking mechanisms will be replaced. Should a key audit reveal less than 100 percent accountability **Tenant** will immediately notify the ASC.

Framework of Responsibility for Access Control Infrastructure

This language from the tenant security agreement of a CAT II airport provides a more detailed outline of access control measures. This overview is complemented by specific instructions for each of the different access control mechanisms, which are outlined in the next two subsections.

Tenant Access Control Overview

- Individuals without a valid Airport ID are not allowed to be left alone, in tenant facility areas with unrestricted access points to the AOA.
- Tenants are required to train their employees to, report unauthorized or suspicious individuals, activities, or items in the AOA, and secure the following access points:
  - Tenant Doors and Gates providing unrestricted to AOA
    - These doors are secured by the tenant through the use of a lock and key system, cipher lock or a TSCAS approved by the Airport.
    - Locks corresponding to unaccounted keys and/or locks that malfunction will immediately be re-cored by tenant.
    - During tenant business hours, these doors are monitored by employees with valid Airport ID to the AOA to ensure no unauthorized access and/or alarmed to control unauthorized use and access to the AOA.
    - When not in use, these doors are secured by the tenant.
  - Vehicle Overhead Doors and Gates
    - These doors are secured by the tenant through use of a lock and key system, cipher lock, or a TSCAS approved by the Airport.
    - These doors are either kept closed and secured or monitored by employees with valid Airport ID to the AOA when open and in use.

5.1.1 Lock and Key Control Systems

Lock and key control systems at airports run the gamut from pen and ink systems to more sophisticated key control programs. While the preferred access control is through automated ACS, the age and physical layouts of many airports make use of automated ACS impractical for some access control points that are required to be secured. Generally, key control of tenant facilities is maintained at the individual facility level. The usual exception is for common access gates; because those gates usually open onto common areas, the airport generally maintains control over them.

The key control process varies widely among airports. Many airports with standard lock and key systems have pen and ink key logs as the basis for their key controls. Others use semi-automated Excel-based spreadsheets. Automated systems for key and lock control are available, but none of the airports interviewed for this research indicated using that type of system. Most of the key control systems operated by tenants were audited on an annual or semiannual basis by the airport.

SAMPLE LANGUAGE

The example provisions below delineate airport and tenant responsibility for operation and maintenance of lock and key and cipher lock systems.

Tenant Responsibility for Key Control

This language from a tenant security plan template for a CAT II airport outlines the responsibilities of tenants with respect to key control.

Tenant Key System (TKS)

Tenants are to control their lock and key systems, which allow unrestricted access to the AOA, by conforming to the following minimum criteria.

The **Tenant** will ensure key holders whose keys have been lost or stolen report the loss or theft to **Airport** Operations immediately.

- The **Tenant** will replace or re-core or replace all locks with unrestricted access to the AOA whenever a single key is reported lost, stolen or otherwise unaccounted.
- **Tenants** are responsible for notifying **Airport** Operations regarding unserviceable locks on access points providing unrestricted access to the AOA.
- The **Tenant** will ensure the return of all keys issued by the tenant when an individual no longer needs unescorted access to the AOA. Keys providing access to airport AOA will only be issued to individuals issued a valid airport ID for AOA.
- The **Tenant** will ensure that only the words “DO NOT DUPLICATE” or “RESTRICTED” along with control numbers and letters that are key holder specific are stamped on each key, and logged by date, key number and issued key holder. No other identifier is used on the keys.
- The **Tenant** will audit keys to access points providing unrestricted access to the AOA at least once annually. A record of the audit must be maintained for at least twelve (12) calendar months including date of audit and name of the person conducting audit.
- The **Tenant** will ensure employees report any lost or stolen keys immediately to the **Tenant**.
- The **Tenant** will maintain un-issued keys in a secure area with access limited to designated key custodians who have an airport approved badge for the AOA.
- The **Tenant** will maintain records of all keys issued including total keys maintained for each lock, key holder name, key serial number, issue date, return date, or date lost.
- The **Airport** monitors tenant lock and key control programs by auditing record keeping, at least once annually, and auditing access points.

See Appendix A for a listing of all doors and gates.

Tenant Responsibility for Combination and Cipher Locks
This language from a tenant security plan template for a CAT II airport outlines the responsibilities of tenants with respect to combination and cipher locks.

Tenant Security Combination/Cipher Locks

Tenants are required to control their doors or gates, which allow unrestricted access to the AOA, and are secured by a cipher lock by conforming to the following minimum criteria.

- Ensure cipher lock combinations and codes are provided only to **Airport** ID badge holders with authorized unescorted access AOA.
- Immediately change lock combinations and cipher lock codes when the combination/code has become compromised or when a person no longer requires unescorted access.
- Unserviceable locks will be immediately reported.
- Maintain a record of the date of last combination/code change, the names and **Airport** ID badge numbers of individuals issued the combination/code for each access point providing unrestricted access to the AOA.
- Train individuals issued the cipher code/combination to not share the code/combination.
- **Airport** monitors Cipher Lock programs by reviewing record keeping, at least once annually, and observing access points.

See Appendix A for a listing of all doors and gates.

5.1.2 Automated Access Control Systems

The preferred method of access control is an automated ACS, which is common in airports and tenant facilities. Most airports operate significant portions of their facilities under a centralized ACS. At some airports, the tenant facilities are linked to those systems, but often they are operated as standalone automated ACS.

The research found that in tenant agreement situations, most tenants wanted control over access to their facilities. However, access to common-use gates, and sometimes even exclusive-use gates, is routinely maintained on the common automated ACS operated by the airport. Where EAAs were in place, the automated ACS is most often operated and controlled by the tenant.

The existence of automated ACS greatly facilitates the ability of airports to monitor access activity for the tenant. Where the automated ACS is under the direct control of the airport, the airport can readily access data for the purposes of inspection and audit. Where the automated ACS is tenant-operated and controlled, measures should be put into agreements to ensure the airport can receive the reports and data necessary to assess tenant access practices.

The types of ACS vary widely from airport to airport; they often also vary within airports, between the airports and their tenants. The hardware and software used to operate these systems also vary widely.

Some airports have sought to homogenize their automated ACS by establishing standards for future tenant installations of automated ACS and outlining specifications for compatible systems. Other airports require tenants to seek airport approval for any automated ACS they might seek to deploy.

Where the automated ACS is centralized and controlled by the airport, issues of new installation, repairs, and maintenance cost should be addressed in tenant agreements. Where the tenant installs its own automated ACS, provisions need to be made to ensure access by select airport personnel, such as security and operations personnel.

SAMPLE LANGUAGE

The example provisions below delineate airport and tenant responsibility for operation and maintenance of automated ACS.

Tenant Responsibility for Automated ACS

This language from a CAT I airport outlines the general responsibilities of tenants in maintaining ACS (automated and non-automated). This example addressing tenant detail is found in the facility access plan executed by each tenant.

General

The **Airport** reserves the right to require the **Tenant** to upgrade its system to comply with all Federal or State regulations as amended from time to time from the Federal government or to interface with the Port's system.

a. An emergency access is required by the **Airport's** Regulations. An override must be provided for all access control or cipher locking systems for Police and Fire emergency use.
b. The **Tenant** shall bear the cost of any future tie-in of the **Tenant's** system to the **Airport's** for any requirement which is mandated by Federal Law or Regulation to interface the two systems. Any requirement over and above that required by Federal Law or Regulation shall be mutually agreed upon by both parties.
c. **Tenant** shall develop and implement security procedures for all locks in **Tenant's** Exclusive Area with secured area access points, employing a tightly controlled key issuance and retrieval system. Keys must be numbered consecutively and stamped DO NOT DUPLICATE. In the event of a lost key or non-return of a from an employee terminated for adverse reasons, the lock core must immediately be changed and a new key issued. If the **Tenant** has reason to believe the employee may pose a threat to the airport or air carrier operations, the **Tenant** must notify the Primary Airport Security Coordinator or the Airport Duty Manager **(XXX) XXX-XXXX** via telephone immediately upon awareness and in writing within 24 hours.

This language from a tenant security plan template for a CAT II airport outlines the responsibilities of tenants with respect to automated ACS.

Tenant Security Computer Access System (TSCAS)

Tenants are required to control their Tenant Security Computer Access System (TSCAS), which allow unrestricted access to the AOA, by conforming to the following minimum criteria.

- Require the return of all access control media issued by the tenant when an individual no longer needs unescorted access to the AOA.
- Tenant access control media providing unrestricted access to airport AOA will only be issued to individuals issued a valid airport ID for AOA.
- The **Tenant** will ensure access control media has a unique individual serial number.
- The **Tenant** will audit tenant access media to access points providing unrestricted to the AOA at least once annually. A record of the audit must be maintained for at least twelve (12) calendar months including date of audit and name of the person conducting audit.
- The **Tenant** will require employees to report any lost or stolen access media and deactivate access media immediately.
- The **Tenant** will maintain un-issued access media in a secure area with access limited to authorized **Airport** ID badged individuals.
- The **Tenant** will maintain records of all access media issued including total access media maintained for each lock with unrestricted access to the AOA, access media holder name, access media serial number, issue date, return date or date lost.
- **Airport** monitors TSCAS programs by auditing record keeping, at least once annually, and auditing access points and the TSCAS.

See Appendix A for a listing of all doors and gates.

Comprehensive Automated ACS Requirements

One CAT X airport has created a comprehensive standards-based approach to managing the Automated Access Control Program for all airport facilities, to include those operated by tenants. The language below is the introduction to the standards document and the outline of the substantive requirements These standards focus on future developments of facilities at the airport.

The standards for Access Control Systems (ACS) at **Airport** are the responsibility of the **XXX** County Aviation Department Security Division. These standards will be included in any future plans for critical infrastructure and access control systems at **Airport**.

The Access Control System shall function as an electronic access control system and shall integrate alarm monitoring, CCTV, digital video, ID badging and database management into a single platform. ACS shall function as a one-stop gateway for all the access control needs. A modular and network-enabled architecture shall allow maximum versatility for tailoring secure and dependable access and alarm monitoring solutions.

Table of Contents

5.2 Signage

Posting and maintaining signage at access points to restricted areas like the AOA, Secured Area, SIDA, and along perimeter fences is frequently addressed in tenant security agreements. It is a mandatory requirement for EAAs and ATSPs, although the methods for addressing signage vary greatly. Some airports provide signage and simply require the tenants to maintain it. Other airports place the burden of creating signage on the tenant. In some cases, airports will simply specify the language that tenants must place on the signage they post. Whatever method the airport chooses to address this issue, the matter of posting and maintaining signage at access points and along fence lines is something that should be considered in tenant agreements.

SAMPLE LANGUAGE

The example provisions below delineate airport and tenant responsibility for signage. Airports should consider outlining responsibility for posting and maintaining signage, and address control over the language in signage.

Tenant Responsibility for Maintaining Signage

This language from a CAT X airport EAA outlines signage requirements for access points. This language could be adapted for non-EAA agreements where signage responsibilities are passed to the tenant.

> **Tenant** will maintain warning signs at all pedestrian and vehicle access points into the **Tenant** Exclusive Security Areas. These signs will warn personnel that only authorized access is allowed.

Approval Process for Signage

This language found in the rules and regulations of a CAT I airport requires tenant compliance with airport standards for signage.

> **Signage and Advertisements**
>
> Signage must be consistent with the applicable County Code of Ordinances, Advertising and Solicitation. Signs, advertisements, notices, circulars, and/or handbills may not be posted, displayed, or distributed without the prior written permission of the County and with an applicable permit. The posting of advertisements on County property shall conform with established County policies and/or directives.
>
> A. Any signage shall comply with any and all requirements of the Airport's Sign Design Guidelines, Requirements and Policies document.
> B. Airport management shall have the right to remove or relocate any such sign, advertisement, notice, circular, and/or handbill posted, displayed, or distributed.

This excerpt from the safety and security handbook of a CAT X airport requires airport approval for signage.

> **Posting Signs Prohibiting Access**
>
> Airport tenants with access to airport Security areas on their property will follow these Rules and Regulations by posting signs approved by the Board which prohibit access leading into airport security areas.

5.3 Lighting

Lighting around tenant areas is an important security consideration; well-lit areas help to reduce criminal activity. While most airports do not address the issue of lighting in their tenant security agreements, it is not unheard of. Airports should consider including language requiring tenants to maintain adequate lighting of their tenant areas, along with a measurable description of the lighting requirements, is something airport should consider.

SAMPLE LANGUAGE

The example provision below specifies lighting requirements for tenant areas. While not commonly addressed in tenant security arrangements, establishing a baseline lighting requirement should be considered.

Common Lighting Standard
This approach by a CAT X airport establishes a common lighting standard for all AOA areas.

> AOA lighting shall be up to a minimum standard. The minimum standard for lighting in these areas is 1 foot-candle.

5.4 Fencing

Fencing is a common requirement for airports, and generally applies to portions of areas occupied by most tenants. Generally, the perimeter fencing is installed by airports, but in certain instances installation can be a tenant responsibility. Many airports have established standards for height and types of fencing that can be installed. Additionally, maintenance of perimeter fencing or other fencing to secure regulated areas is critical to ensure continuous security. Airports should consider addressing fencing in their tenant security agreements, including specifications for fence installation and responsibility for fence maintenance and repair.

SAMPLE LANGUAGE

The example provision below addresses compliance with airport fencing standards. Allocating responsibility for maintenance and repair are also important matters to consider.

Common Fencing Standard
This approach by a CAT X airport requires tenants to utilize airport-established standards in connection with the maintenance of fencing.

> Airport Security has a perimeter fence standard. Any modifications made to the AOA fence by the tenant, shall be made to the Airport fence standard under the responsibility of the tenant. The fence standards can be found in the Airport Standards for Perimeter Fences and Gates document.

5.5 Clear Zones

Maintaining clear zones around fencing is also an important part of perimeter security. Many tenant security agreements include requirements that clear zones be maintained along tenant fence lines that constitute part of regulated areas.

SAMPLE LANGUAGE

The language below provides an example of standards for maintaining clear zones.

Tenant Responsibility for Maintaining Clear Zones
This approach by a CAT X airport establishes a common standard for all airport clear zones.

> The perimeter fence line, to include buildings and fences, must have a clear zone as described in the Airport Security Program. A clear zone provides an area that is free from obstructions which can inhibit viewing the perimeter for vulnerabilities during an inspection or provide an unauthorized individual to gain access. The clear zone is a minimum distance of six (6) feet from any building, fence, or other structure that is used as the perimeter boundary. Additionally, **XXX** County Code of Ordinances, Section 39-77(9) must be adhered to in regard to landscaping and clear zones.

5.6 CCTV

Most airports operate some form of central CCTV system. The systems in tenant facilities are not typically included in the airport system, but common areas like ramp areas and gates often are. The primary constraint to CCTV coverage is usually physical infrastructure like power and cabling.

Most airport tenants operate their own separate camera systems within their facility, which frequently cover areas around their facilities, including ramp areas of the airport. Airport access to images from these cameras is generally limited to requests for information after an event or incident. Access to real-time feeds from tenant systems was not found at any airport in the research. The processes for seeking access to images from tenant systems were rarely formalized. However, most airports believe there would not be any problem obtaining access to images if necessary.

While most airports have not instituted significant controls over CCTV, some larger airports have focused considerable attention to control over the types of technology that tenants can employ, as well as access to, and use and dissemination of images generated by CCTV systems. One airport has compiled detailed standards for tenant CCTV deployments so that images can easily be shared with the airport.

SAMPLE LANGUAGE

The example provisions below concern the operation of CCTV systems. The language addresses a wide range of issues, including dissemination of images and SSI implications, technical specifications for camera system development, and comprehensive use and governance guidelines. The language addresses the use of tenant video as an independent system, as well as part of a unified or federated system at an airport. It also addresses airport access to tenant video for investigative purposes, and airport control over CCTV images, particularly images of common areas like taxiways and ramps.

Governance of Tenant CCTV Systems
This approach by a CAT I airport requires tenant-operated CCTV be subjected to TSA control in dissemination.

> **Use of Camera and other Recording Devices**
>
> Airport tenants who operate video camera systems or other recording devices that record portion of the Sterile Area or other areas of the Airport are subject to TSA regulations, must not release any recording or images obtained from these systems to the public without complying with TSA Sensitive Security Information (SSI) guidance on the release of such recordings or images. The classification of SSI or other SSI Guidance materials can be found on the Department of Homeland Security's website.

Comprehensive Provisions on CCTV Technical Standards

One CAT X airport has created a comprehensive standards-based approach to managing CCTV use for all airport facilities, including those operated by tenants. The language below is the introduction to the standards document and the outline of the substantive requirements. These standards are focused on future development of facilities at the airport.

The CCTV system is another core subsystem of an overall Electronic Security System (ESS). It is the collection of cameras, recorders, switches, keyboards, and monitors that allow viewing and recording of security events. The CCTV system can be integrated with the Access Control System (ACS) and Intrusion Detection System (IDS) and may be centrally monitored at the Dispatch Center or Airport Operations Center monitored by security personnel at an individual facility. Uses of CCTV systems for security services include several different functions as described below.

The **XXX** County Aviation Department operates and maintains a comprehensive integrated CCTV network to serve airport wide needs at **Airport**. This network serves the security and surveillance needs for the **Airport** Security, Operations, Facility Maintenance Divisions, TSA, CBP and **XXX** County Sheriff's Office LEO and Fire Rescue Departments.

Table of Contents

8.18 Maintenance and Service Level Standards
8.19 CCTV Viewing Capabilities by Agency
9. Project Related
9.1 Specifications for CCTV Workstations

Comprehensive Provisions on Tenant CCTV Use and Governance

One CAT X airport has an extensive policy on the use of CCTV cameras and equipment at tenant facilities. This language from the airport rules and regulations offers a comprehensive approach to controlling tenant use of CCTV. The regulations govern CCTV deployment, security, and the use and sharing of CCTV images.

Tenant Video Monitoring and Recording Devices

A. Installation or Removal of Video Monitoring and Other Recording Devices

No video monitoring or other recording devices may be installed or removed by any Airport tenant or permittee in or around the Airport premises without prior written authorization from the Aviation Security unit. To obtain authorization for CCTV camera installation or removal, tenants and permittees must submit an application, specifying the following:

- Field-of View (FOV) screenshots
- Video monitoring/recording device model and specifications
- Camera layout drawing
- Security infrastructure and plan to prevent unauthorized access

The use of Pan-Tilt-Zoom (PTZ) security cameras by tenants and permittees in any secured or AOA area is strictly prohibited and no video monitoring and/or recording device may be installed or focused in a manner that depicts/records security checkpoints, or doors that provide access to any area on Airport premises that, in the sole and exclusive discretion of the Airport Director or his designee, is deemed to present a potential risk to Airport security. All subsequent changes or modifications to tenant and permittee video monitoring and/or recording device use must be submitted to Aviation Security in writing and approved prior to executing modifications.

B. Remote Viewing and Authorization Access

No video monitoring and/or recording device data may be streamed or otherwise transmitted on a wireless network unless the wireless network is equipped with WPA2 security. Real-time access to all footage must be available to the Aviation Security unit at all times. No tenant or permittee shall release any video monitoring and/or recording device footage from cameras/devises without prior written authorization from the Aviation Security unit and, if deemed appropriate, the TSA. Remote access to video monitoring and/or recording devices in secure areas will not be permitted unless explicitly authorized by the Airport Director.

All forms of video footage, whether real-time or stored, must be password protected. Passwords must comply with the Airport's Password policy.

C. Inventory of Video Monitoring and Other Recording Devices

All tenants and permittees shall provide Aviation Security with an inventory of existing video monitoring and/or recording devices and security plans, including all of the following:

- Device manufacturer, model and specifications
- Field-of-view
- Data retention time
- Placement of video monitoring and/or recording devices
- Remote access usage
- Written security plan detailing how unauthorized access will be prevented

Comprehensive Provisions on Airport and Tenant CCTV Use and Governance

A similar detailed approach to CCTV regulation is exemplified by the policy below taken from another CAT X airport. It addresses both tenant use of their own CCTV systems and access to the CCTV system operated by the airport.

CCTV Security Surveillance System Policies and Guidelines

1. **Introduction**
   - A. This Operating Directive will serve to provide the policies and procedures to be adhered to by all DOA personnel, vendors, concessionaires, contractors, businesses, airlines, or any other persons or entities who have access to **Airport's** CCTV (Closed Circuit Television) Security Surveillance System. CCTV is used to enhance security, safety and the quality of life by integrating the best practices of "virtual policing" with state-of-the-art technology.
   - B. The Security Division will be the regulatory entity regarding **Airport's** CCTV Security Surveillance System. The Security Division will be responsible for the CCTV Security Surveillance System to include the installation and use of cameras; use and operation of the VMS (Video Management System); placement, use and operation of associated VMS workstations; approval of who will have access of any type to the CCTV Security Surveillance System; the preservation of selected video footage; the viewing of the video footage; and, the preparation of CDs or other digital media and to allow viewing of selected video (collectively referred to as "CD").
   - C. Violations of this Operating Directive will be addressed by the Security Division and DOA Employee Services.

2. **Installation of Cameras and Recording Systems**
   - A. Any installation of camera equipment (including recording equipment), either independent of, or to be added to **Airport's** CCTV Surveillance Systems, by any DOA personnel, or any vendors, concessionaires, contractors, businesses, airlines. or any other persons or entities, must first be approved by the Security Division.
   - B. The approval of any installation of cameras will address the following, but not be limited to:
     - a. The name and type of camera(s).
     - b. The number of cameras.
     - c. The location of the camera(s).
     - d. The reason for the camera(s).
     - e. The views that the camera(s) will be looking at.
     - f. And other questions and considerations regarding the particular requested CCTV installation and operation.
     - g. The submission of a PCA (Project Concept Approval) for any project involving the CCTV Security Surveillance System, including the installation of CCTV Cameras or platform/workstations, does not eliminate the requirement for the Security Division to approve any such project or work prior to that project or work beginning.
     - h. Any integration between the CCTV Security Surveillance System and the Access Control System at **Airport** must be approved by the Security Division. Due to the high security element of this type of integration and operation, and the critical SSI regarding this type of integration and operation, only the Access Control provider will facilitate this type of integration with the direction of the Security Division and the Airport Control Center.
3. **Use of Airport's VMS and Related CCTV Surveillance System**
   - A. This Operating Directive serves to provide policies and procedures which will address the use of the VMS.
     - a. The VMS (collectively referred to as the "platform") will be made accessible through computer workstations.
     - b. The placement and location of the workstations; who will be authorized to use them; and what level of operational and administrative capabilities any particular workstation or operator has, will be determined and approved only by the Security Division.

B. This Operating Directive serves to provide policies and procedures which will address the use of the CCTV and related recording capabilities associated with the platform. CCTV cameras are used to enhance security, safety and the quality of life by integrating the best practices of "virtual policing" with state-of-the-art technology.

C. **Airport** is using CCTV to monitor areas throughout the airport in order to deter crime and to assist in providing for the security and safety of individuals and property. Any diversion of security technologies for other purposes would undermine the utilization of these resources for achievement of critical safety goals and is therefore strictly prohibited.

D. Examples of legitimate safety and security purposes for CCTV monitoring include, but are not limited to:

a. Protection of individuals, property and buildings
b. Confirmation of alarms or events
c. Patrol of public areas
d. Monitor aircraft movement
e. Investigation of incidents at the TSA Check Points
f. Investigation of criminal activity
g. Emergency/ Incident response
h. Investigation of smoke, fire, or flooding
i. Monitoring Security K-9 activity
j. Security training

E. The use of CCTV will be conducted in a professional, ethical and legal manner. Personnel involved in monitoring will be appropriately trained and supervised in the responsible use of this technology. CCTV monitoring will be conducted in a manner consistent with all existing policies, including the Non-Discrimination Policy, the Sexual Harassment Policy, and other relevant facility policies.

F. Monitoring individuals based solely on characteristics of race, gender, ethnicity, sexual orientation, celebrity status or recognition disability, or other protected classifications is prohibited.

G. CCTV will not target or focus on the faces of persons engaging in First Amendment demonstration activities unless there is a reasonable indication of a threat to public safety or of engagement in criminal activity.

H. Information obtained through video monitoring will be used exclusively for safety, security, or law enforcement purposes. Recorded images will be stored in a secure location that is accessible only to authorized staff. Use of video for entertainment or personal use is strictly prohibited.

I. It is strictly prohibited to use a cell phone, or any other device to photograph or record images which are visible on any CCTV Security Surveillance System Monitors or platforms.

J. Access to view Security Surveillance System monitors or to operate the CCTV Platform is strictly limited to staff with authorization to do so.

K. Recorded material will not be sold or used for commercial purposes.

L. Operator logon accounts and other audit features will be used to ensure a clear operator audit trail is maintained. This enables tracking of abusive use of CCTV assets back to the individual who violated a policy.

4. **Selected Video Preservation Policy and Procedures**

A. This Operating Directive will serve to provide the policies and procedures for Security Division Personnel to adhere to regarding the preservation of selected video footage, the viewing of the video footage, and the preparation of CDs or other digital media; to allow viewing of selected video (collectively referred to as "CD"). It is intended to facilitate the preservation of selected video footage which may depict information relevant to reported emergencies, criminal activities, property damage, sick or injured persons, or similar incidents, provided that the Security Division receives timely notice of said incidents.

B. The Department of Aviation has installed a security video surveillance system at **Airport**. Video obtained through the security surveillance system is not retained on a regular basis and is not a public record. The surveillance system is intended to provide real time monitoring of certain

locations at the Airport and does not create permanent records. The video surveillance system equipment has limited, short term recording capacity which varies, depending upon the equipment used, from one (I) to four (4) months. When any particular equipment's retention reaches capacity, it commences to record new video images over whatever may have been previously recorded. The DOA endeavors to extract and retain specific video relating to a specific incident, or to a specific location during a specific time period, upon reasonable request, if what was requested was actually recorded and if the request is made in a timely manner which allows recovery of the specific video while it is still in the system's short term storage.

C. Only Security Division Personnel are allowed to preserve CCTV video footage; copy CCTV video footage; export CCTV video footage; or, produce CDs containing CCTV video Footage.
   a. Exceptions
      i. The TSA is allowed to export CCTV video footage and produce CDs containing CCTV video footage, related to a TSA investigation of activity having taken place at the TSA Check Points or TSA baggage handling areas. TSA will notify the Security Division of such export of CCTV video footage.
      ii. (ii) Security Division Management may grant temporary authorization to other DOA or Law Enforcement personnel to export CCTV video footage or prepare CDs containing video footage, when there is a critical time element involved.

D. The Security Division will only preserve selected video footage or prepare a CD if it is made aware in a timely fashion of an incident warranting the preservation of the selected video footage video, or if a specific request is made, or a subpoena or notice of litigation hold (collectively referred to as "Requests") is served in a timely fashion upon the Security Division. Requests may be submitted by: Airport divisions, including the Director's Office, Airport Control Center (ACC), Risk Management/Safety; Terminal Ops; Airside; Landside; Public Affairs and Marketing; Employee Relations; stale and local agencies, including **XXX** Police Department and the District Attorney's Office; federal agencies, including the U.S. Attorney, FBI, TSA, CBP, and ATF; a private attorney's office; airlines; tenants; or by any other outside individual, agency, or entity. Any Request may be subject to review by the TSA for a determination of Sensitive Security Information content prior to its release. The number and exact location of security surveillance cameras is Sensitive Security Information and will not be disclosed to unauthorized parties.

E. Requests to preserve selected video footage, to view video footage and/or to prepare a CD of such selected video footage may be made either directly to the Security Division or through the Airport Control Center. The Security Division has the sole authority to approve the preservation of selected video footage, to approve the viewing of the video footage, or prepare a CD. The following policies and procedures will be followed in response to the above cited situations.

5. **Requests Made Directly to the Security Division**

   A. When the Security Division is contacted by any person, agency or entity with a Request for selected video footage preserved, to view video footage, or prepare a CD the Security Division will have to be advised by the requesting party of the details including the type of situation the video footage is for and the date time and location of the incident.

   B. If an incident report or other written report of the incident or activity is available, that report will be forwarded to the Security Division. If the requesting party knows which cameras recorded the video footage, that information will also be passed on to Security. If the specific camera(s) are not known by the requesting party, Security will check with the ACC to determine if they are aware of which camera(s) were used to record the incident. If the requesting party or the ACC are not aware of which camera(s) may have recorded the incident, Security will search all the available and pertinent cameras and try to locate the requested video footage.

6. **Requests Made Directly Through the ACC**

   A. When the ACC receives a Request for video footage to be preserved, to view video footage of the incident, or prepare a CD, the ACC will email Security with the identity of who is requesting the video footage; the type of situation the video footage is for; the date & time of the incident; and, which camera(s) recorded the footage of the incident. Security will then locate the camera(s) and footage and: a) save the footage to the DOA Confidential Drive: and b) when specifically requested, transfer the footage to a CD (or other digital media).

a. Exceptions:

i. The ACC may in fact allow certain entities, while in the performance of their official duties and while conducting ongoing investigations, to respond to the ACC and view video footage. These entities are limited to **XXX** Police; any other city, state or federal law enforcement; **XXX** Fire; Airfield Operations Coordinators; OSHA Inspectors ONLY when looking into an accident on an escalator or elevator; and DOA Risk Management & Safety. All other requests to view video footage must be approved by Security 24/7. If the ACC personnel are unsure if they should allow the viewing of any video footage by any entity or individual, they should contact security (**XXX-XXX-XXXX** or **XXX-XXX-XXXX**) 24/7.

ii. If Security is able to determine that video exists which responds to the Request, Security will then: a) save the footage to the DOA Confidential Drive, and b) when specifically requested, transfer the footage to a CD (or other digital media). Security will then notify the requesting entity when the CD is prepared. Subject to the necessity of TSA review before release, if applicable, Security will then notify the requesting entity when the CD is prepared. The requesting person or entity shall sign a receipt containing the name of the person or entity, date, and a brief description of the content of the CD when the CD is delivered to the requestor. That receipt will be kept on file with the Security Division.

B. Other factors regarding the preservation of video footage and the preparation of a CD (or other digital media) include but are not limited to:

a. The duration of how long video footage remains available to be located, preserved or transferred to a CD is determined by the particular video surveillance equipment and its recording system components. This is an Information Service area of expertise and is not a Security function or area of specific knowledge and expertise.

b. Video footage preserved or saved to the Confidential Drive contains, at least in part, selected video footage which may depict information relevant to reported emergencies, criminal activities, property damage, sick or injured persons, or similar incidents. Any such footage may be determined to be "Airport Emergency Documentation Records," as defined in the **XXX** State Local Government Retention Schedule. Such records have a minimum retention period of three (3) calendar years from the date of last action pursuant to state public records retention law. Such records shall not be removed or deleted after the minimum retention period without the authorization of the Security Division, after consultation with the District Attorney's Office.

c. Security personnel will notify the DA's office whenever a subpoena or other formal written request for video footage regarding legal proceedings is received by the Security Division.

d. Only Security Division personnel will preserve video footage on the Confidential Drive or prepare a CD; and, only Security Division personnel will release any video footage or CD. Under no circumstances will any department, division, or individual, other than Security Personnel release video footage to any person, agency or entity.

e. No video footage regarding DOA employees will be preserved or transferred to a CD unless Employee Services is made aware of the request and approves the request.

f. If a request is received by the Security Division, which is regarded as unusual or out of the realm of the normal and standard requests, Security personnel will discuss and review the request before any action is taken with the video footage.

g. Security Division Management will determine when the Director will be made aware of any video footage request. For example, requests for video footage by Federal Attorneys, local or national media, international entities, etc., would warrant the Director being advised.

SECTION 6: AGREEMENT PREPARATION, CREATION, AND REVIEW

The majority of airports have no formal process or policy for the preparation of agreements related to or incorporated in the ASP, regardless of agreement type. Generally, such agreements are initiated by airport security personnel seeking to address the modification or expansion of existing tenant agreements. In rare instances, the tenant has suggested the implementation of a program.

6.1 Drafting Agreements

The preparation of security agreements related to the ASP generally involves a draft agreement being circulated back and forth between the airport, usually security personnel, and the tenants. While some airports choose to create templates, the vast majority do not; in general, airports create agreements on a case-by-case basis. Often this is the result of complicated leasing agreements in place, the relatively small number of agreements and lack of frequency in negotiating them, or other factors outside of security. Airports interested in creating templates should reach out to TSA or other airports for suggested agreement formats. Sample language, which may also help with template creation, is included in Appendices B, C, and D.

TSA approval is required to introduce agreements or measures into the ASP, so a strategy to engage the TSA is essential. The TSA needs to be involved at some stage in the negotiations. Some airports include the TSA early in the process, but most wait until after preliminary negotiations have been conducted with the tenant.

Often, airport security personnel have little input with respect to provisions in leases, or rules and regulations. Those provisions are typically addressed by airport counsel and, in the case of leases, real estate or property personnel. Most leases created in this manner include general form language with respect to security requirements. However, in some airports the development of a close working relationship between the security and the properties or facilities management departments has led to inclusion of stronger security provisions in leases and regulations.

The preceding chapters describe many of the security-focused areas that may be included in an airport's agreement with their tenant. When drafting an agreement, the airport should consider creating a checklist that outlines areas the agreement should cover, which can be marked as completed during the development phase. The checklist to the right is a sample that an airport could use as a starting point.

Does the document cover:

- ☐ Facility Audits
  - ☐ Auditor
  - ☐ Schedule (or random)
- ☐ Document Audits
  - ☐ Auditor
  - ☐ Schedule (or random)
- ☐ Floor Plans/Layout
- ☐ Equipment Maintenance
  - ☐ Maintenance of security equipment
  - ☐ Scheduled maintenance
  - ☐ Backups/redundancy
- ☐ Liability
  - ☐ Airport's responsibility
  - ☐ Tenant's responsibility
  - ☐ Consequences/penalties
- ☐ Special events
  - ☐ Construction
  - ☐ Events

6.2 Creating a Template

Airports should consider creating a template that can be easily updated and modified for each type of agreement. Templates are standardized documents with common text, layout, structure, and formatting, which can be customized to meet the needs of the specific agreement while maintaining an established standard. All modern word processing software programs have the ability to create and use a document template. Templates are not to be confused with samples of old contracts; templates are a separate file type that can be used to create a new document without altering the original template.

Using old documents as templates presents risks. A document used for a different lease period or tenant may no longer be compliant with TSA and airport regulations, or may include language only applicable to one tenant or space. Also, creating new documents from existing documents reduces the possibility of a common foundation, since each new document may include elements of any number of previous documents.

Effective templates should allow changes to the definition and description of secure areas, changes in agreement ownership, and other common changes to be made easily and quickly. Suggestions for templates and general document management include:

- Establish a naming or numbering convention for documents, or use an existing convention, and display the document number (including version information and effective date) in the header or footer of every page.
- Make customizable areas such as organization name obvious to users. This can be done by using all capital letters in brackets (e.g. [NAME]) or by using different text colors or font emphasis such as bold or italics – black is often used for "locked" or unchangeable text while blue or italics is used to indicate modifiable text. Consider what may happen if the document is printed in black and white when choosing to use colors to indicate modifiable text or other important document characteristics.
- Add space at the bottom of each page for signatures/initials and date – should one part of the agreement need to be changed, only the affected pages would need to be updated and replaced. The date block would provide a method of tracking changes.
- Create appendices for information which changes regularly rather than including it in the core document. It is much easier to change and get change approval for an appendix than for main document changes. Also consider including any material deemed SSI in appendices to avoid making the entire document subject to SSI constraints.
- Attach current point of contact information to the agreement as a letter or memorandum. This is a common change to agreements and should be easy to update.
- Create a cover letter which indicates the current version of the document and revision dates. Include a table in the cover letter to summarize changes as the document is edited. This creates an audit trail from the current version to prior versions.
- The language in the template should be comprehensive; it is much easier to delete irrelevant information than to add information.
- Ensure the template file name indicates that the file is a template for ease of identification. Adding the word "Template" to the file name is one option. When added as a prefix to the file name, this facilitates keeping all the template files together in a sorted file list.

6.3 Maps and Floorplans

Many airport tenants have dedicated facilities for their operations (cargo, FBOs, etc.), but many airports have no floorplan or map of the facility in their records. Creating and maintaining an "as-built" floorplan of the facility allows airports to quickly identify altered areas during inspections and audits. Many airports have found changes to access controlled doors, loading docks, and office areas they had not been informed of and that did not appear on floorplans or facility maps. In some cases, these changes created a potential security issue. In others, the TSA noticed the discrepancy during their audit. Additionally, the airport needs an accurate floorplan to provide to first responders in the event of an emergency.

Maintaining an accurate and current understanding of tenant use of leasehold space can be of critical importance for compliance. As an example, at one airport, the tenant modified one of their hangars, which resulted in a change to the AOA boundary. Such activity can result in the imposition of federal fines and penalties.

6.4 Amending Agreements

Some airports have indicated that they signed agreements with their tenants covering terms of 20 years or more. This was often a result of a greenfield airport attempting to recover from the large investment of building the airport with some guarantee of return on investment. However, some of these airports have found themselves unable to alter these agreements to more appropriately reflect current industry trends and evolving airport needs. Altering these leases when they expire may prove difficult for some airports, especially if the tenant provides a significant portion of the airport's revenue and brings in many of the airport's customers. Long-term contracts should be considered carefully due to the future complications that they may cause. Agreements should include provisions or language that allows the airport to alter the terms to reflect changes such as updated federal requirements or new technology.

Occasionally, tenants plan events within their facilities, such as construction projects, corporate parties, or fundraising events. Some airports that have been in this situation created a temporary amendment to the tenant agreement that changed the security procedures and protocols for the duration of the event. An airport LEO was often posted at the facility during the event to make sure there were no issues.

6.5 Agreement Audits

Many airports maintain several tenant agreements at once, and some even have multiple agreements with the same tenant. Maintaining these agreements can prove difficult if they are not properly logged or are kept as physical copies rather than digital. Some airports utilize a spreadsheet to help manage the agreements, identify points of contact, and identify agreements that are nearing expiration. Document management systems offer a more robust alternative to spreadsheets and filing cabinets. Software like this would enable the airport to scan or upload each page of an agreement, create tags to enable filtering, and create searchable documents to quickly find information that may be buried within hundreds of pages. Modern document management systems often create and maintain a keyword-searchable index of their content as well.

This option requires purchasing or subscribing to the software, which may be cost prohibitive for some airports. However, for airports managing many agreements it may pay for itself in reduced labor cost.

At least one airport has created a centralized network-based solution to help them prepare, execute, maintain, access, and update their agreements. This airport maintains at least six EAAs and multiple agreements with other tenants. It was important to them to be able to manage these agreements virtually for efficiency.

It is important to review tenant agreements regularly to ensure the information they contain is up to date, and to capture any new or updated requirements. Reviewing agreements with the tenant gives them an opportunity to indicate changes they may have made since the last review, such as technology or equipment upgrades. Annual reviews are the most common at airports but, at a minimum, each agreement should be reviewed at the end of its life cycle. Agreements should also be reviewed when new regulations that affect the agreements are released by the TSA or other relevant regulating agency/body.

As part of the auditing process, attention should be paid to assessing changes that have occurred during the audit period. This would include changes resulting from TSA regulatory actions, developments in the security environment, and/or operational imperatives in the tenant's organization. The need for regular auditing and adjustment is important for all security agreements, but particularly for EAAs and ATSPs. The auditing process should include education and training on the process necessary to keep tenant agreements updated and accurate.

In the dynamic airport environment, it is important to ensure that tenant agreements are regularly reviewed and refreshed. Development and execution of a schedule of regularly occurring agreement audits is a way to ensure both airport and tenant personnel are familiar with their security agreements, and that those agreements are accurate and current.

REFERENCES

Airport tenant security program requirement. (2009). 49 CFR § 1542.113.

Alaska Administrative Code, Title 17. (2006). *Chapter 45. Rural Airports.* *http://www.touchngo.com/lglcntr/akstats/aac/title17/chapter045.htm*.

Breed, London. (2019). *San Francisco International Airport Rules and Regulations.* Airport Commission. https://www.flysfo.com/sites/default/files/media/sfo/about-sfo/Rules_and_Regulations_10-15-19.pdf.

Code of Ordinances No. 20-7, Supp. No. 79. (2020). *Chapter 4 – County Airports.* Milwaukee County, Wisconsin. https://library.municode.com/wi/milwaukee_county/codes/code_of_ordinances?nodeId=MICOCOGEORVOI_CH4COAI.

Exclusive area agreements. (2009). 49 CFR § 1542.111.

Faith Group, LLC. (2017). *PARAS 0010: Guidance for Protecting Access to Vital Systems impacting Airport Security.* National Safe Skies Alliance, Inc.

General Mitchell International Airport. *Rules and Regulations.* *https://www.mitchellairport.com/application/files/1915/4836/4404/MKE_Rules_and_Regulations_12.04.17-final_2018.pdf*.

Government Accountability Office. (2012). Screening Partnership Program: TSA Should Issue More Guidance to Airports and Monitor Private versus Federal Screener Performance, *GAO-12-208*.

Kenton County Airport Board. (2019). *Rules and Regulations of Kenton County Airport Board relating to the Operation and Control of the Cincinnati/Northern Kentucky International Airport.* *https://www.cvgairport.com/docs/default-source/default-document-library/cvg-rules-and-regs.pdf?sfvrsn=8*.

Lam Lha. (2019). *PARAS 0020: Strategies for Effective Airport Identification Media Accountability and Control.* National Safe Skies Alliance, Inc.

Los Angeles World Airports. (2016). *Certified Service Provider Program. https://www.lawa.org/-/media/lawa-web/lawa-airport-operations/files/cspp-brochure-jun-16.ashx*.

Metropolitan Airport Authority. (2018). *Airport Rules and Regulations*. https://www.qcairport.com/assets/files/files/Rules%20&%20Regulations%202018.pdf.

Office of the Comptroller of Currency. (2013). OCC Bulletin 2013-29, *Third-Party Relationships: Risk Management Guidance.*

Transportation Security Administration. *Best Practices Guide for Non-DHS Employees and Contractors. https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf.*

Transportation Security Administration. (2014). *Airport Security Program and 49 CFR 1542 Implementation Guidance*.

Transportation Security Administration. (2017). *Security Guidelines for General Aviation Airport Operators and Users*.

APPENDIX A: ASSESSMENT WORKSHEET TO IDENTIFY SUITABILITY FOR EAA/ATSP

Purpose

The purpose of the assessment worksheet is to help airport decision makers identify whether a centralized, non-regulatory agreement or decentralized, regulated approach is best suited for their situation.

Directions

Rate each of the 20 statements using the scale below:

Strongly Disagree – 1 **Disagree – 2** **Neutral – 3** **Agree – 4** **Strongly Agree – 5**

Add the scores of all statements and write the total at the bottom of the table.

Results

If the total score is between:

20 – 50 Consider a centralized, non-regulated approach. As stated in this document, there are several unique options to choose from, including revisions to existing leases or modifications to your ASP.

50 – 70 Consider either a centralized or decentralized approach.

70 – 100 Consider a decentralized, regulated ATSP or EAA. You would choose an EAA if you are working with an airline or an ATSP if you are not.

Next Steps

Once you know which type of agreement would work best, consider using the sample language in the examples provided throughout this document as well as the Tables of Contents structures in the following appendices to get started.

#		Score 1-5
Airport Focused		
1	Centralized control is important to the airport's overall philosophy of security operations.	
2	Centralized security operations are a key part of the airports overall risk mitigation strategy.	
3	Centralized security operations are an important part of the Airport's security culture.	
4	The cost of centralized security does not impose a fiscal burden in the airport.	
5	The airport has little experience and practice in collaborative operational programs with tenants.	
6	The airport has sufficient resources to perform security operations in tenant areas.	
7	The airport's security support infrastructure (e.g., ID media management) and access control have sufficient capacity to meet tenant security requirements.	
8	The airport has sufficient physical infrastructure to support centralized security operations for tenant areas.	
9	The geographic layout of tenant operations on the airport does not lend itself to an independent security operation.	
10	TSA enforcement will not focus away from the airport and onto tenants if control is decentralized.	
Tenant Focused		
11	The tenant's operation is not unique and does not lend itself to an independent security operation.	
12	The tenant's security strategy does not adequately align to airport concerns.	
13	The tenant's organization does not have a strong security culture.	
14	The airport's relationship with the tenant does not seem predisposed to collaborative security operations.	
15	The tenant's level of security skill and experience is low.	
16	The tenant does not have sufficient staff/resources to conduct an independent security operation.	
17	The tenant's level of technical capability to establish and or maintain security infrastructure requirements in the tenant area is low.	
18	The tenant lacks the financial capability to establish and or maintain security infrastructure requirements in the tenant area.	
19	The tenant's interest level in operating an independent security operation is low.	
20	The tenant's interest level in direct TSA oversight with additional accountability to the airport is low.	
	TOTAL	

APPENDIX B: EXAMPLES FROM DIRECT FEDERALLY REGULATED AGREEMENTS

Currently, the only types of federally regulated agreements are EAAs and ATSPs. This appendix provides examples of Tables of Contents from EAAs and ATSPs currently in place at U.S. airports or from templates of those documents. These examples are not meant to be comprehensive for every airport or tenant, but are presented as a typical outline of the contents of an EAA or ATSP.

Airports using the example outline for their own agreements should consult their airport legal department to review the document.

Text in gray boxes is taken from the respective documents
Text in ***bold italics*** is commentary from the team that is designed to highlight significant features
Text in **blue** is meant to be replaced with the airport-specific information

EAAs

This is a detailed long form for an EAA used by a CAT I airport

Clearly specified definitions

- Purpose of Agreement (compliance with 1542.111, 1542.203, 1542.205, 1542.207, 1542.211, 1542.213, 1542.303, 1544.231, Full All-Cargo AOSSP)
- Terms of Agreement
- Organization of Security Personnel and Responsibilities
    - Point of contact(s) (if contacts are different for airline, EAA, or physical infrastructure)
    - Backup contacts
    - Security contractor(s), employed contact(s)
- Access Points and Security Control Procedures
    - Access control description
    - Access control systems
    - Access control points
        - Vehicle Gates/Entry
        - Pedestrian Gates/Entry
        - Special use areas
        - Tractor trailer gates
        - Vendors/Contractor procedures
        - Airport EAA line of demarcation
    - Procedures for security breaches detection and communication
    - Temporary amendment process
    - Patrols
    - Lighting
    - Fencing
    - Access Media (employee IDs, vendor IDs, temporary IDs, aircraft maintenance, airline crew, airline support personnel, TSA personnel)
        - Displaying ID media
        - Challenging requirements
        - Issuance and control of ID media
    - Vehicle ID and Control
    - Escort procedures
    - Lock and key control
    - Notification of Security Issues
    - Proof of compliance

- Special Procedures
  - Law Enforcement
  - Special Events
  - Other Air Carriers (1544 & 1556)
  - Construction Projects
- Maps
- Signage Examples
- ID Media samples
- EAA Training Program Curriculum
  - SSI
  - Challenge Procedures
  - ID Media Display
  - Suspicious Activity
  - Individual accountability
  - Fraud
  - Confidential Info
  - Insider Threat
- Special Operations
  - Snow Removal
  - Special Events
  - Construction Projects

This is a short form for an EAA used by a CAT X airport.

AIRPORT SECURITY PLAN—***References the airport's Airport Security Plan***

I. 1542.111 – EXCLUSIVE USE AREA
   a. Defines the Exclusive Area and includes a schematic.
   b. Specifies Tenant is required to apply measures specified in the agreement
   c. Requires tenant notification of changes in the Excusive area

II. 1542.201 – TENANT'S RESPONSIBILITY FOR SECURITY OVER THE SECURED AREAS ADJOINING TENANT'S EXCLUSIVE AREA
   a. Measures for controlling access
   b. Detection of and Response to Unauthorized Presence
   c. Establish and Carrying Personal ID
   d. CHRC and STA Requirements for Unescorted Access
   e. Security Training
   f. Signage

III. 1542.207 – TENANT ACCESS CONTROL SYSTEMS
   a. Ensures Access Only by Authorized Personnel
   b. Denies Access When Authority is Withdrawn
   c. Differentiates Area Access Rights
   d. Escort Procedures Established

IV. 1542.211 – IDENTIFICATION SYSTEMS

V. HOLD HARMLESS/INDEMNIFICATION

VI. TERMINATION
   a. RIGHT OF INSPECTION & AMENDMENT (Compliance with the Agreement)
   b. RIGHT OF INSPECTION & AMENDMENT (Access Points)
   c. FINES

d. GENERAL
   i. Tenant Upgrade of Systems
   ii. Emergency Access
   iii. Cost Allocation for Tie-Ins
   iv. Lock and Key Control
   v. Notice of Change Conditions
   vi. Entire Agreement

ATSPs

This is a short form for an ATSP used by a CAT III airport.

1 Applicability
2 General
3 Security Related Incidents
4 Security Measures Assumed by Tenant
5 Airport Operator ATSP Audit Measures
6 Penalties for Noncompliance
7 Protection of SSI
8 Condition Change or Alternate Security Measures
9 Transportation Security Administration Inspection Authority
10 Attachment A: Tenant Facility Map
11 Attachment B: Identification Media
12 Signature Page

This is a long form for an ATSP created by a CAT X airport.

A. Contact Page
B. General Requirements 49. C.F.R. 1542.101
   A. Incident and Suspicious Activity
   B. Right of Inspection
   C. Termination of Program for Cause
   D. Actions for Non-Compliance
   E. Monetary Penalties by the TSA
   F. Security Briefings
C. Standard Definition of Terms
D. Approvals and Amendments 49 C.F.R. 1542.1051
E. Description of Building
   A. Facility
   B. Building Diagrams
F. Security of the SIDA/Secured Area
   A. Security Inspection
   B. AOA Perimeter Fence including Temporary Fence
   C. Clear Zone

G. Changed Conditions Affecting Security
- A. Planned changes
- B. Unplanned changes

H. Access Control 49 C.F.R. 1542.207
- A. Manually operated Vehicle Gates
- B. Lock and Key Control
  - i. Airport-controlled access points
  - ii. Tenant-controlled access points
- C. Computerized Access Control System (CACS)
  - i. Airport Security ID Card Revocation Procedures
  - ii. SIDA/Secured Area Access Points
  - iii. Turnstiles
- D. Response to SIDA/Secured Area Doors and Emergency Door Alarms
- E. Rail Line

I. Identification Systems 49 C.F.R. 1542.211 and 1542.103(a) (8)

J. Escort Procedures
- A. Challenge procedures

K. Security Directives and Information Circulars

L. Signature Page

Attachment 1 – XXX Airport Security Standards & Guidelines
- Attachment 1A – Specifications for all SIDA/Secured AOA Perimeter Fences
- Attachment 1B – Vehicle Inspection Guidelines
- Attachment 1C – Lock and Key Usage
- Attachment 1D – Alarm Response Procedures
- Attachment 1E – Security Guard Procedures for the Stop List
- Attachment 1F – Signage
- Attachment 1G – Procedures for Access Control at the Rail Line
- Attachment 1H – Protection of Sensitive Security Information (SSI)
- Attachment 1I – Additional Standards/Specifications if any

Attachment 2 – Airline/Airport Tenant Procedures
- Attachment 2A – Building Site Plan
- Attachment 2B – List of All Active SIDA/Secured Access Points
- Attachment 2C – List of All Inactive SIDA/Secured Access Points
- Attachment 2D – Measures for Clear Zone
- Attachment 2E – Patrol Procedures
- Attachment 2F – Airline/Airport Tenant's CACS System
- Attachment 2G – Key Control Log Sheet
- Attachment 2H – Contract Security Guard Services
- Attachment 2I – Other Specific Procedure (1) used in Building X
- Attachment 2J – Other Specific Procedure (2) used in Building X
- Attachment 2K – Other Specific Procedure (3) used in Building X

APPENDIX C: EXAMPLES FROM AD HOC FEDERALLY REGULATED ARRANGEMENTS

This appendix outlines the content of tenant security programs that are regulated to some degree by the TSA, generally under the auspices of an ASP. They are often incorporated as part of the ASP but are not mandated to be included in the ASP. Once incorporated in the ASP, however, their requirements become ASP requirements.

The following sample language is by not meant to be comprehensive for every possible scenario an airport may encounter. It is presented to offer airports examples of language for each section of an agreement. Airports looking at this language are encouraged to adapt these samples to their own needs and requirements by changing words, using some sections, and discarding others.

Airports using the sample language in their own agreements should consult their airport legal department to review the document.

Text in gray boxes is taken from the respective documents
Text in ***bold italics*** is commentary from the team that is designed to highlight significant features
Text in **blue** is meant to be replaced with the airport-specific information

LOCATION-BASED TENANT SECURITY PROGRAMS

The following table of contents from a template of a location-based tenant security program was developed by a CAT X airport to improve security of FBO operations

TENANT FACILITY STANDARDS
TABLE OF CONTENTS

This location-based tenant security program was developed by a CAT X airport to improve security of FBO operations. While the introduction notes a focus on FBO operations, it could easily be adapted to address other tenant operations. The airport also created a template that outlines security technology and other requirements for tenant facilities; the table of contents for that program is also included below.

TENANT SECURITY PROGRAM

SECTION I – INTRODUCTION

Purpose
Tenant herein known as "Tenant" has developed this security plan to enhance the security of fixed base aviation operations at the Airport. Although General Aviation (GA) Fixed Base Operators (FBO's) are not regulated by the Transportation Security Administration (TSA), the Security Guidelines for General Aviation FBO Operators issued by the TSA for GA were reviewed during plan development. The Tenant must ensure that the measures contained in this Tenant Security Program are implemented to provide for the safety and 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.

Distribution
The following agencies are in possession of this FBO Security Program.

- XXX County Aviation Department;
- The Transportation Security Administration
- XXX County Sheriff's Office; and
- Tenant Security Coordinator and other personnel with security related responsibilities.

SECTION II – COMMUNICATION

Security Contacts

Primary Point of Contact: name, title and can be reached at XXX-XXX-XXXX during working hours, and XXX-XXX-XXXX after hours.

Secondary Point of Contact: name, title and can be reached at XXX-XXX-XXXX during working hours, and XXX-XXX-XXXX after hours.

Emergency Phone Numbers
The following is a list of all outside emergency contact numbers.

- All Emergencies: **911**
- XXX County Law Enforcement Non-Emergency: XXX-XXX-XXXX
- FBO Operations Control Center (AOCC): XXX-XXX-XXXX
- TSA Coordination Center: XXX-XXX-XXXX
- XXX Airport Security Coordinator (ASC): XXX-XXX-XXXX
- XXX Airport Security Duty-Phone: XXX-XXX-XXXX

Emergency contact information is posted in Tenant hangars, the pilot lounge and on the office bulletin board.

SECTION III – PHYSICAL FACILITY OVERVIEW

General Information

- Address: address
- Contact Numbers:
  - Normal business: XXX-XXX-XXXX
  - 24-hour Emergency: XXX-XXX-XXXX
  - Fax Phone Number: XXX-XXX-XXXX
- Geographical Coordinates:
  - Latitude: XX.XX
  - Longitude: XX.XX

- Hours of Operation: **XXXX - XXXX**
- Average Number of Annual Operations: **XXX**
- Number of Based Aircraft: **XXX**
- Footprint: **in approximate acres**
- Ramps: **identify ramp areas and provide a tenant layout plan/diagram as an attachment**
- Buildings: **list the number and types of buildings (offices, hangars, maintenance shops)**
- Flight Activities: **xxx**

Access Control

- Key Control: **articulate how keys are controlled**
- Vehicles: Vehicle access to the AOA is restricted through gate fencing. Only authorized automobile traffic is allowed on the AOA operating areas. Emergency personnel have been provided a key to all locked gates at the airport.
- Fencing: **XXX** linear feet fencing borders along the north side of Perimeter Road. Fencing is vertical feet chain link fence with one foot of outrigger top-guard.
- Gates: There are **XXX** vehicle gates and **XXX** pedestrian gates.
- Pedestrian Access: **Pedestrian traffic is controlled through...**
- Office Buildings: There is/are **XXX** office buildings at the facility.
    - Office Building **building number**
        - Access Controlled Doors: **xxx**
        - Non-Access Controlled Doors: **xxx**
- Maintenance Buildings: There is/are **XXX** maintenance buildings at the facility.
    - Office Building **building number**
        - Access Controlled Doors: **xxx**
        - Non-Access Controlled Doors: **xxx**
- Hangars: There are **XXX** hangars at the facility. Each hangar is equipped with padlocks on pedestrian doors and a locking system for the main hangar door. Hanger doors are closed and locked when tenants are not present, and aircraft are in the hangar.
    - Hanger 1 **building number**
        - Access Controlled Doors: **number and type of access control system**
        - Non-Access Controlled Doors: **number and type of access control system**
        - Aircraft Capacity: **XXX**
- A layout map is attached in **Appendix 1** showing the fencing, vehicle gates, pedestrian gates, gates and access points, access to hangars and buildings.

Signage

- Tenant has restrictive signs posted at vehicular and pedestrian access points and “No Trespassing” signs are posted along the perimeter fencing.

Lighting

- The facility is well lit with **XXX** lighting.

Closed Circuit Television (CCTV):

- The facility has **XXX** CCTV cameras at the facility that is actively/passively monitored. Recordings are kept for up to **XXX** days.

Fueling

- Tenant conducts fueling operations and has number of fueling point(s) providing types of fuel. Additionally, the Tenant has number fuel trucks that are parked in a secure area. No self-fueling is done at the facility.

SECTION IV – AIRPORT SECURITY AND LAW ENFORCEMENT SUPPORT

Security and Law Enforcement Patrols

- Security and Law Enforcement patrols are conducted by **XXX** Police and provide surveillance, act as a deterrent, and respond to security-related incidents. Both **XXX** Police and Airport Authority Personnel provide 24/7 security and law enforcement patrols at **XXX** Airport. When the security level increases at

the Airport, additional patrols are conducted.

- Other patrol activities will be determined by a collaborative effort in conjunction with **XXX** Police and Airport Authority Personnel as deemed appropriate.

SECTION V – INCIDENT MANAGEMENT

Incidents, Suspicious Activity, and Threat Information

- **Define incidents, suspicious activities, and threat information. Tenant** should contact local law enforcement immediately by calling 911.
- If the activity is not an emergency situation, but requires review, the activity should be reported using the Airport Police Non-Emergency number and the **Tenant** Security Coordinator's number.

Bomb Threats, or other Threat of Sabotage

Upon direct or referred receipt of bomb threats, threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations, **Tenant** will immediately evaluate the threat in accordance with this security plan and report to the appropriate authorities on the contact list. Contact 911 immediately.

Tenant Emergency Contact Information

	Name	Phone Number	Second Number
Tenant Security Point of Contact			
Tenant Manager			
Tenant Commission Chair			
Police Department		911	Nonemergency Number:
County Sheriff		911	Nonemergency Number:
Fire Department		911	Nonemergency Number:
County Emergency Manager			
State Department of Homeland Security			
State DOT Office of Aviation			
AOPA Watch			
Transportation Security Administration (see map for relevant TSA hub)			
Federal Security Director			
Deputy Federal Security Director			
Tenant Security Point of Contact			
Tenant Manager			
Tenant Commission Chair			
Police Department		911	Nonemergency

			Number:
County Sheriff		911	Nonemergency Number:
Fire Department		911	Nonemergency Number:
County Emergency Manager			
State Department of Homeland Security			
State DOT Office of Aviation			
AOPA Watch			

OPERATIONS-BASED TENANT SECURITY PROGRAMS

One CAT I airport had a unique operations-based approach to tenant security. One of the airport's tenants was a primary, but not exclusive, user of ramp space in a congested ramp area of the airport. An EAA was not permitted because the tenant did not have exclusive use for the area. However, this operations-based approached allowed for the creation of a tenant-controlled area during specified operational hours when additional security provisions were met by the tenant.

M1-1 General
This plan establishes the policies, guidelines, and procedures to ensure compliance with 49 CFR Part 1542.203 (Security of the Air Operations Area), Part 1542.205 (Security of the Security Identification Display Area), and the TSA-approved Airport Security Program (ASP), **Appendix M, M-1 and M-2.** In addition, it ensures compliance with the Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP), Section 10.5 (Area Security).

Tenant's Contract Security Provider is responsible for the compliance and implementation of all written Post Orders pertaining to operations within the **Tenant's** designated leasehold space. Any updates to the Contract Security Post Orders shall be coordinated through the Airport's Aviation Security and Public Safety Department for approval, and prior to implementation. The Contract Security Provider/**Tenant** must ensure that on-sight officers are trained in a manner acceptable to the Authority. All Post Orders shall be made available to the Airport and TSA for inspection or review upon request.

Security Operations are defined as any activity that occurs within the **Tenant's** designated leasehold space which requires the use of Vehicle Gate **XXX** for the movement of any vehicle or person; and involves any operation requiring the provisions of this plan.

NOTE: Although this plan provides policies, guidelines, and procedures for the security of the **Tenant** Operations Area, the Aircraft Operator (**Tenant**) shall comply with all pertinent sections of the TSA-approved Airport Security Program (ASP).

LIST OF APPENDICES

M1-2 Tenant Operations Area
Description of the areas covered in the appendix including a schematic of the area

M1-3 Identification (ID) Media
Describes the Airport ID and **Tenant's** IDs that can be used in the area to meet SIDA requirements.

M1-4 Access Control and Security-Personnel and Vehicles
Establishes the temporal framework for opening and closing the area for exclusive tenant use and the attendant security measures

A. Commencing Security Operations-Conditions of Appendix Are Activated
Outlines the measures that the tenant must undertake to open the area (principally the staffing of specified security posts and initiating a series of procedures and logging requirements to ensure area security) and notifications to the Airport Communications Center

B. Terminating Security Operations-Conditions of Appendix No Longer in Effect
Outlines the process for closing the area—closing security posts and sweeping the area.

C. Area Control
Establishes requirements for positive control of the area—display of badges, challenge. incident reporting.

M1-5 Escorts and Escorting
Describes the process for escort within the area during operational periods, including ID media requirements and escort ratios.

M1-6 Vehicle access to Tenant Operations Area
Describes the protocols for vehicle access by both vehicles with and without unescorted access authorizations including the delineation of permitting requirements and placards (cross referencing to vehicle permitting provisions of the ASP).

M1-7 Plan Amendments
Outlines the process for amendment of the plan once TSA has approved it.

M1-2 Accountability
Reiterates the requirement for compliance with other applicable federal regulatory provisions.

APPENDIX D: EXAMPLES FROM NON-FEDERALLY REGULATED ARRANGEMENTS

This appendix outlines the content of tenant security programs that are not regulated by the TSA. Rather, these types of agreements are generally regulated at the state, county, or city level.

The following sample language is by not meant to be comprehensive for every possible scenario an airport may encounter. It is presented to offer airports examples of language that may be included in a non-federally regulated agreement. Airports looking at this language are encouraged to adapt these samples to their own needs and requirements.

Airports using the sample language in their own agreements should consult their airport legal department to review the document.

Text in gray boxes is taken from the respective documents
Text in **blue** is meant to be replaced with the airport-specific information.

LOCAL REGULATORY PROVISIONS—Airport Rules and Regulations

AIRPORT SECURITY REQUIREMENTS (NARROW)

This is an example of a narrowly focused security regulation that principally addresses concerns over security breaches in federally regulated areas of the airport. This language comes from the rules and regulations of a CAT II airport. In addition to the issues directly addressed below, the regulations contain provisions addressing badging, access, escort, and challenge procedures. Specifically addressing tenant responsibilities, this regulation places responsibility for access control squarely on the tenant.

Security Responsibilities of Employees and Other Persons

(a) No person may:
   i. Tamper, interfere with, compromise, modify, attempt to circumvent, or cause a person to tamper, interfere with, compromise, modify, or attempt to circumvent any security system, measure, or procedure.
   ii. Enter, or be present within, a Secured Area, AOA, SIDA, or sterile area without complying with the systems, measures, or procedures being applied to control access to, or presence or movement in, such areas.
   iii. Use, allow to be used, or cause to be used, any airport-issued or airport- approved access medium or identification medium that authorizes the access, presence, or movement of persons or Vehicles in Secured Areas, AOAs, or SIDAs in any other manner than that for which it was issued by the Airport Authority.

(b) Airport Authority Police Officers and other local law enforcement officers have the power and authority to enforce laws, ordinances, rules and regulations within the airport boundaries.

(c) Tenants are responsible for the security of all Aircraft and other private property entrusted to their care on the AOA or other locations within their tenant-leased areas of responsibility.

(d) Tenants and tenant employees are responsible for controlling access to doors, gates and other passageways between the AOA and the land side of the airport through their lease areas.

(e) A breach in security caused by a tenant or tenant employee that results in a TSA or Director of Aviation finding of negligence will be cause to review, suspend, or withdraw access privileges, impose additional training requirements and/or impose other penalties as provided by these Rules and Regulations and the Airport Security Program.

AIRPORT SECURITY REQUIREMENTS (GENERAL SECURITY REQUIREMENTS)

Some airports combine generalized provisions for regulatory compliance with several more provisions looking at specific areas of conduct. In this example the CAT X airport outlines general requirements combined with over seventy safety and security related offenses. Some of those include issues like: unauthorized entry and inspection; piggybacking; vehicle and nonvehicle escorts; clear zones; badge-related requirements; preventing unauthorized access; security of access points; reporting rule violations; bypassing security screening; and challenge procedures.

Commercial Activity -- Federal, State, and/or Local Laws or Regulations – Every Person using the Airport shall comply with all federal, state, and/or local laws, regulations, orders and/or decisions, including those of executive, legislative or judicial agencies or bodies, now or hereafter in effect, and applicable to the Person's use of the Airport.

Every tenant and/or lessee of the Board, or any other Person doing business with the Board or at the Airport, shall comply with all federal, state, and/or local laws, regulations, orders and/or decisions, including those of executive, legislative, or judicial agencies or bodies, now or hereafter in effect, and applicable to that tenant's, lessee's, or other Person's operations at the Airport.

Safety and Security Regulations – Adherence to Airport Security Directions.
All Persons will obey lawful orders and directions of Airport Police Officers or other Persons responsible for insuring compliance with these Rules and Regulations. All orders or directions will be consistent with the Airport Master Security Program, Board Rules and Regulations, and applicable state, federal and local laws.

AIRPORT SECURITY REQUIREMENTS (SPECIFIC SECURITY PROVISIONS/ENFORCEMENT)

This represents a more comprehensive approach to regulatory control over security measures at a CAT X airport. The provisions of the regulation attempt to address non-SSI related security measures in the ASP. Some of the more unique regulatory measures are included in their entirety.

Only the security regulation and a portion of the enforcement provisions are reprinted here. The enforcement regulation contains a detailed schedule and classification of offenses, and outlines a schedule of penalties. It also has a detailed set of monetary and nonmonetary penalties relating to badging. For the sake of brevity, other measures have been redacted, indicated by the present of three asterisks (***).

RULE 7.0
AIRPORT SECURITY

1. **General Provisions**
   - **Priority.** Safety and security are the Airport's first priorities. The requirements of this Rule 7 are critical to the safe and secure operation of the Airport. All personnel working and doing business on Airport property must comply with this Rule at all times and model the significance of safety and security for co-workers, passengers, and members of the public.
   - **Definition of Restricted Area.** For the purpose of this Rule 7 only, any area on Airport property, whether within a building or terminal or on the ramp or airfield area, including but not limited to all Secured Areas, Sterile Areas, Restricted Areas, and the Air Operations Area (AOA), shall be referred to collectively as the "Restricted Area."
   - **Airport Security Program.** This Rule 7 includes the non-Sensitive Security Information (SSI) requirements set forth in the Airport Security Program (ASP) issued by the Director under 49 C.F.R. 1542.
   - **Enforcement.** Any person who violates this Rule 7, compromises Airport security, or creates or engages or participates in any unsafe, unsecure, or hazardous condition or activity at the Airport may have his/her access privileges immediately revoked on a temporary or permanent basis at the sole discretion of the Airport (see also Rule 7.3 and Rule 14.4). Any person or entity responsible in

whole or in part for any security violation shall also be responsible for any resulting cost, including but not limited to any fine imposed by a regulatory agency or remediation of property damage or personal injury.

2. Security Badges

A. Airport ID Badge

Persons who work or do business on Airport property on a permanent or long-term (longer than 30 days) basis must have an Airport-issued identification in the form of an Airport ID badge. An individual holding an Airport ID badge may also be referred to as "badged personnel."

1) **Attainment: *****
2) **Expiration: *****
3) **Return: *****

B. "T" Badge

Persons who work or do business on Airport property on a temporary basis (30 days or fewer) must have an Airport-issued Temporary or "T" badge.

1) **Attainment: *****
2) **Frequency/Duration: *****
3) **Limited Access/Escort Required: *****

3. Airport ID Badge Holder and Tenant Employer Security Responsibilities / Access Control Procedures

All badged personnel have an affirmative duty to maintain a secure Airport. Airport tenants, contractors, and permittees are responsible for ensuring that their employees, suppliers, contractors, subcontractors, and all other businesses and entities providing services on Airport property comply with Rule 7 of these Rules and Regulations.

A. Badge Display and Use ***

B. Security Screening ***

C. Access to Restricted Area ***

1) Piggybacking/Tailgating: ***
2) Keys and Locks: ***
3) Secure Doors and Gates: ***
4) **Report False Alarm:** Badged personnel are required to immediately report any self- activation of a door alarm to the Security Operations Center at **(XXX) XXX-XXXX**.
5) **Damage: *****
6) **Unauthorized Access:** Badged personnel must report any unauthorized person(s) in a Restricted Area and any potential security violations to the Airport's Communications Center by dialing 911.

D. **Restricted Area Duty to Challenge**

Badged personnel must conscientiously observe the presence of an Airport ID badge on other employees. Every Airport ID badge holder must ensure the following: ***

E. Drug and Alcohol Prohibition

1) **Prohibited Substances:** ***
2) **Prescription Drugs: *****
3) **Working under the Influence:** No Airport ID badge holder may enter or remain in a Restricted Area if the individual is in any way impaired as a result of ingesting substances referenced in this Rule 7.3, including prescription drugs.

F. **Tenant's Use of Armed Guards, Armored Vehicles, Armed Courier Services**

Tenants using armed guards and/or armored courier services to, for example, transport currency or high value items or to service automated teller machines, must assure that that its service provider comply as follows: ***

1) **Badge Required: *****
2) **Vehicle access: *****

3) **Parking: *****

G. Security Testing

4. Transporting Items into the Restricted Area

A. TSA Prohibited Items

B. Procedures to Transport Prohibited Items into the Restricted Area

All Airport ID badge holders, tenants, or contractors requiring knives, tools, and/or or heavy equipment to perform their job duties or for their business operations in a Restricted Area are required to comply with the following procedures.

1) Food and Beverage Inventory Items: ***
2) Inspection of Merchandise and Consumables: ***
3) Tools (Temporary Non-Inventory): ***
4) Transport of Heavy/Oversized Prohibited Items: ***

5. Tenant Video Monitoring and Recording Devices

A. Installation or Removal of Video Monitoring and Other Recording Devices ***

B. Remote Viewing and Authorization Access ***

C. Inventory of Video Monitoring and Other Recording Devices ***

6. Other Restricted Areas

A. Clear Zone ***

B. Water Perimeter Zone ***

C. Utility Tunnels ***

7. Prohibitions

No person or entity may:

1) Tamper or interfere with, compromise, modify, or attempt to circumvent any security system, measure, or procedure implemented under the Airport's ASP and TSA Regulations under 49
   a. C.F.R. § 1500, et seq.;
2) Enter, or be present within, a Restricted Area without complying with the systems, measures, or procedures being applied to control access as defined in the Airport's ASP and TSA Regulations under 49 C.F.R. § 1500, et seq.; or
3) Use or allow to be used any Airport-issued access medium or identification system that authorizes the access, presence, or movement of persons or vehicles in Restricted Area in any unauthorized manner.

8. Quality Standards Program ("Qsp")

The Airport Commission adopted the Quality Standards Program ("QSP") to enhance safety and security at the Airport. The purpose of the policy is to ensure that the service providers offer the highest level of quality service to the Airport community, and to enforce the minimum standards for safety, health, hiring, training, wages and benefits, and equipment standards for the airline service provider employees. ***

RULE 14.0
ENFORCEMENT AND ADMINISTRATIVE APPEAL PROCEDURE

1. **Enforcement Generally**

The Airport, through any authorized Airport Commission employee or any Law Enforcement Officer, may cite infractions of these Rules and Regulations to any individual or business entity by issuance of a verbal or written Admonishment or a written Citation.

2. **General and Administrative Fines**

Any person or business entity violating or otherwise engaging in prohibited conduct under these Rules and Regulations may be subject to general and/or administrative fines as provided under this Rule 14. If the violator is an individual employee or agent of an Airport tenant, permittee, or contractor, the fine may be assessed against the employer/tenant, permittee, or contractor at the Airport's discretion.

All violations and respective fines may be cumulative of each other (one citation may contain multiple fines) and shall be imposed in addition to and neither exclusive nor preclusive of any other civil or criminal federal, state, or local fine or penalty under the law or of any other remedy available to the Airport under the law or under a lease, permit, or contract. An infraction may result in multiple charges to a tenant, permittee, or contractor and/or its employee in the form of fines, fees, and charges under the applicable lease, permit, or contract. For example, a commercial ground transportation operator may receive a citation for speeding under the **State** Vehicle Code and a fine under these Rules and Regulations.

The Airport reserves all rights with respect to its enforcement of these Rules and Regulations and of its leases, permits, and contracts.

The following list references violations by Rule and Regulation Rule but may not be exhaustive of the entire Rules and Regulations as may be amended from time to time. The headings or titles above the Rules are solely for purpose of convenience and not intended to limit the scope of a listed Rule. In the event a prohibited activity described in the Rules and Regulations does not appear in the list below, the associated fine shall be charged under Category A.

LEASE AGREEMENT

AIRPORT SECURITY REQUIREMENTS

The language below is from the lease and use agreement for a CAT X airport. It was revised in 2020. The agreement is detailed and imposes significant compliance responsibilities on the tenant. The lease requires direct tenant compliance with federal mandates, and specifically covers cost issues requiring that compliance. Additionally, the language addresses compliance with security plans prepared by the city and approved by federal authorities. There is a provision requiring tenant airlines to take adequate measures to maintain security of leased premises, and even a requirement for execution of an EAA.

The lease calls out required compliance on a number of topics, including security training, badging, vetting of ID media holders, and screening and inspection. Provisions in the lease place the tenant on notice that security requirements may affect business operations and costs, and impose direct responsibility on the tenant for the payment of any fines and penalties related to its operations including fines and penalties levied by or against the city. The agreement also allows for the imposition of user fees in connection with badging or use of city-controlled access control systems. While these provisions apply only to airline users, with the exception of the EAA requirement, they likely can be related to other tenant leases.

Security and Payment of Fines for Violation of Federal Regulations

1. Airline acknowledges that security is of primary importance at the Airport and that security requirements are likely to change during the Term. Airline, its officers, employees, representatives, agents, servants, subtenants, consultants, contractors, successors, assigns and suppliers and those under its control, shall comply with security measures
    a. required of Airline by the FAA or the TSA or by the City in accordance with applicable requirements of the FAA or the TSA or their authorized successor(s) or (b) contained in any Airport master security plan approved by the FAA or the TSA or their authorized successor(s). Airline shall comply, at its own expense, with the TSA's security requirements applicable to Airline at the Airport including, but not limited to, employee security training, badging, criminal background checks, access control, screening and inspections. Airline shall cooperate with the TSA on all security matters.
2. Compliance with such security measures and requirements shall not relieve Airline of its responsibility for maintaining proper security for the above-noted items, nor shall it be construed as limiting in any manner Airline's obligations with respect to all applicable federal laws and regulations and its duty to undertake reasonable action to establish and maintain secure conditions at and around the Premises. To comply with TSA requirements, Airline hereby agrees to execute a reasonable exclusive area

agreement pursuant to 49 C.F.R. 1542.111 with the City in form and substance which is reasonably acceptable to the parties. Airline accepts security responsibility to use best efforts to prevent unauthorized access to the Premises. Airline shall be responsible for preventing unauthorized persons from gaining access to the restricted areas of the Airport through the Premises during times and to the extent that Airline has control of the Premises.

3. Airline understands and agrees that security requirements may affect Airline's Air Transportation Business operations and costs. Airline shall be strictly liable for the payment of any fines assessed by the City or the payment of (or reimbursement of City for any payments of) any civil penalties assessed against City or Airline relating to security and resulting from the negligence or intentional acts of omission or commission of Airline's officers, employees, representatives, agents, servants, subtenants, consultants, contractors, successors, assigns and suppliers and those under its control, and Airline shall be solely and fully responsible for any and all breaches of security and the consequences thereof resulting from the negligence or intentional acts of omission or commission of its officers, employees, representatives, agents, servants, subtenants, consultants, contractors, successors, assigns and suppliers and those under its control.
4. The City may impose and Airline agrees to pay a reasonable nondiscriminatory cost-based user fee, if any, for the privilege of using identification cards or badges to gain access to the Airport security access control system.

This language is from a standardized template for airport leases across a large state-operated system. The language provides simple terms requiring compliance with federally mandated security programs. It shifts compliance cost to the tenants, and also provides for reimbursement for fines or penalties imposed on the airport as a result of tenant conduct. The language provides clear guidance for reimbursement and responsibility for the remediation costs. The lease provisions apply only to federally imposed requirements, and not those related to state or local regulations that cannot be related to a federal requirement.

1. The Lessee will coordinate any Airport security matter with the Lessor. If the Airport is operated under 49 CFR Part 1542 (Airport Security) and 14 CFR Part 139 (Airport Certification), the Lessee will comply with all applicable requirements of the Lessor's Airport Security Program, Airport Certification Manual, and Airport Emergency Plan. Upon written notice from Lessor, Lessee will, at its sole expense, promptly correct any violation or omission under the Airport Security Program or Airport Certification Manual within the time specified in the notice.
2. If the Transportation Security Administration (TSA), the Federal Aviation Administration (FAA) or any other federal, state or local government agency fines or otherwise imposes a monetary penalty on the Lessor or requires the Lessor to remediate or mitigate any condition for a violation of a statute, ordinance, or regulation, and if the violation is caused by or based on, all or in part, an act or omission by the Lessee or someone acting on the Lessee's behalf, the Lessee will reimburse the Lessor for the amount of the fine or penalty, the Lessor's costs incurred to remediate or mitigate the condition, and any legal or other associated costs incurred by the Lessor in responding to the violation. The Lessee will reimburse the Lessor for fines, penalties or costs, paid within 30 days after receipt of written notice from the Lessor.

LICENSURE PROGRAM

Rather than focusing solely on a real estate-based approach to regulation, some airports have developed an approach that licenses companies performing services on airport property. These programs require company acknowledgement of obligations in a range of areas, including those that concern airport safety and security. The language below, taken from the licensing program of a CAT X airport, indicates the type of issues commonly addressed in such programs.

DEMONSTRATION OF AIRPORT SERVICE STANDARDS.

Minimum standards include:

- Airport Security
- Vehicle & Equipment Safety
- Experience & Capacity (Core Service Providers)
- Property & Facilities at **XXX** Airport
- Emergency Response Procedure Awareness
- Personnel & Training Requirements
- Wheelchair Services (if applicable)