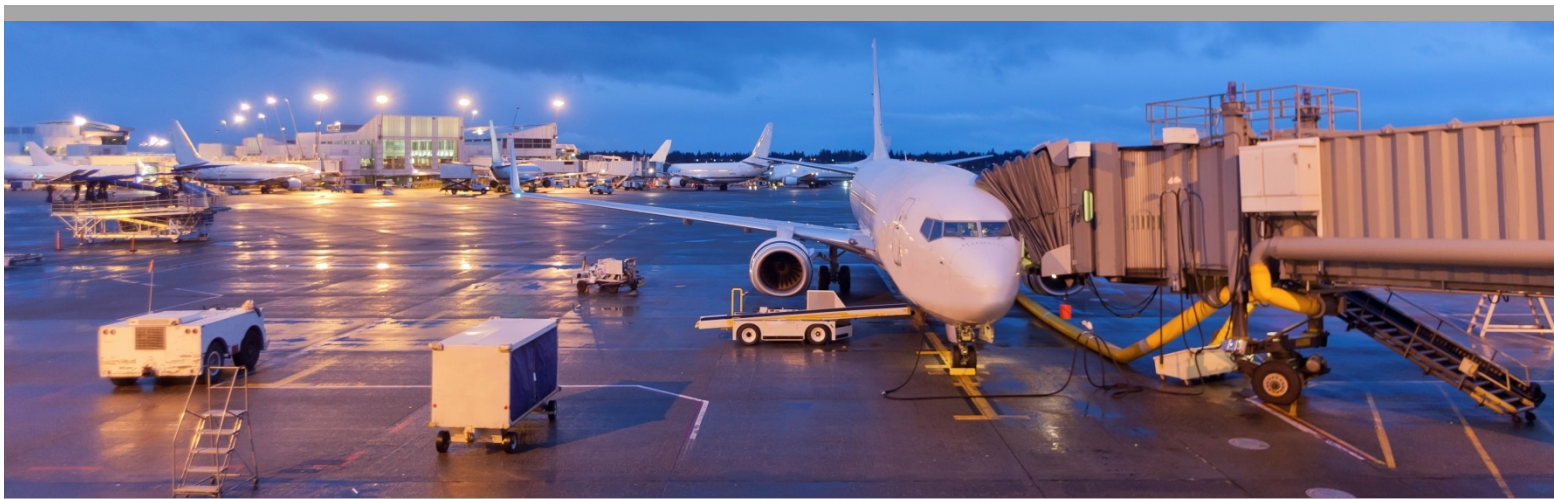




PARAS

PROGRAM FOR APPLIED
RESEARCH IN AIRPORT SECURITY



PARAS 0028

February 2021

Recommended Security Guidelines for Airport Planning, Design, and Construction

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

René Rieder Jr, PSP, CPP, ASC
Burns Engineering
Philadelphia, PA

© 2021 National Safe Skies Alliance, Inc. All rights reserved.

COPYRIGHT INFORMATION

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

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

NOTICE

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

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

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

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

NATIONAL SAFE SKIES ALLIANCE, INC.

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

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

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

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

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

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

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

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

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

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

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

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0028 PROJECT PANEL

Sean Bogart *Gresham Smith*

Shelie Bumgarner *Port of Seattle*

Joshua Cousins *Dallas Fort Worth International Airport*

Aaron Lawrence *Woolpert*

Michael Pilgrim *ISC International Security Concepts*

Jeremy Martelle *CHA Consulting, Inc.*

Dale Mason *Transportation Security Administration*

William Reinhardt *Federal Aviation Administration*

AUTHOR ACKNOWLEDGEMENTS

BURNS ENGINEERING

- René Rieder Jr, PSP, CPP, ASC, Aviation Security Lead
- Suzanne Guzik, Senior Systems Engineering Specialist
- Ivo Krakic, Systems Engineering Specialist
- Sally Salvatorelli, Web Developer/Graphic Artist

KPFF CONSULTING ENGINEERS, INC.

- Sharon Gallant, SE, Principal, Protective Design and Blast SME
- Leslie Duffy, PE, Associate, Protective Design and Blast SME

NEWCASTLE CONSULTING, LLC

- J. Kelly Stewart, President & CEO, Risk Assessment SME

CONTENTS

PARAS ACRONYMS	xi
ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS	xii
HOW TO USE THIS DOCUMENT	xiv
DOCUMENT ORGANIZATION	xv
SECTION 1: INTRODUCTION AND INTENT	1
1.1 Setting the Stage	1
1.2 Applicability	1
1.3 Considerations	2
1.4 Changing Security Concerns and Contingency Measures	3
SECTION 2: PLANNING THE SECURITY DESIGN	4
2.1 Planning for the Design	4
2.1.1 General Security Areas and Boundaries	4
2.2 Initial Project Planning	6
2.3 Security Workshops	7
2.4 Project Definition Document (PDD)	9
2.5 Threat and Vulnerability Assessment (TVA)	9
2.5.1 Reference and Guidance Documents	10
2.5.2 Value of Threat and Vulnerability Assessments	10
2.5.3 Quantitative and Qualitative	10
2.5.4 Methodologies & Approaches	12
2.6 Blast Assessment	13
2.6.1 Reference and Guidance Documents	13
2.6.2 Historic Events	13
2.6.3 Design Challenges	14
2.6.4 Assessment Process	14
2.6.5 Best Practices and Industry Trends	20
2.7 Hostile Vehicle Assessment	20
2.7.1 Vehicle Vector Analysis	21
2.7.2 Site Design	21
2.7.3 Crash Ratings	21
2.8 Basis of Design (BoD)	23
2.8.1 Protection of Sensitive Security Design Information	24
2.9 Planning the Security Design Checklist	24
SECTION 3: AIRPORT SECURITY SYSTEM DESIGN	26
3.1 Physical Security Systems	26
3.1.1 Natural Barriers	26
3.1.2 Physical Barriers	26

3.1.3	Reference and Guidance Documents	28
3.1.4	Design Checklist	28
3.2	Electronic Security Systems	28
3.2.1	Access Control Systems (ACS)	28
3.2.2	Perimeter Intrusion Detection Systems (PIDS)	33
3.2.3	Video Surveillance Systems (VSS)	33
3.2.4	Exit Lane Breach Control Systems	37
3.2.5	Reference and Guidance Documents	37
3.2.6	Design Checklist	37
3.3	Security Operations Center (SOC)	38
3.3.1	SOC System Concept	39
3.3.2	Design Objectives	39
3.3.3	SOC Configurations	40
3.3.4	SOC Infrastructure	43
3.3.5	Other Design Considerations	44
3.3.6	Trends	45
3.3.7	Design Checklist	46
3.4	Baggage Handling System	47
3.4.1	Reference and Guidance Document	47
3.4.2	Design Checklist	47
3.5	Security Screening Checkpoint	48
3.5.1	Reference and Guidance Document	49
3.5.2	Design Checklist	49
3.6	IT Security	50
3.6.1	Information Security and Risk Management	50
3.6.2	Security Design Issues	51
3.6.3	Legal Issues	53
3.6.4	Reference and Guidance Documents	55
3.6.5	Design Checklist	55
3.7	Coordination	55
3.7.1	Communication/IT Systems	59
3.7.2	Electrical/Power Systems	60
3.7.3	Lighting Systems	63
3.7.4	Mechanical Systems	65
3.7.5	Civil Systems	65
3.7.6	Architectural Systems	66
3.7.7	Coordination/Design Checklist	70
SECTION 4: CONSTRUCTION AND HAND-OVER		72

4.1	Security during Construction	72
4.1.1	Existing Security Systems	72
4.1.2	Contractors	73
4.1.3	Work Zones	73
4.2	Testing	74
4.2.1	Sample ACS Door Testing Procedure	75
4.2.2	Sample VSS Testing Procedure	76
4.2.3	Testing Documentation Tools	76
4.3	Training	77
4.3.1	Levels of Training	77
4.3.2	Train the Trainer	77
4.4	ORAT	77
4.5	Owner Acceptance	78
4.5.1	License Transfer	78
4.5.2	Record/As Built Drawings	78
4.5.3	Operation and Maintenance Manuals	78
4.6	Operation	79
4.6.1	Maintenance	79
4.6.2	Life Cycle	80
4.7	Coordination/Design Checklist	80
	APPENDIX A: DEFINITIONS	A-1
	APPENDIX B: ONLINE RESOURCES AND REFERENCES	B-1
	APPENDIX C: AVIATION SECURITY BACKGROUND AND HISTORY	C-1
	APPENDIX D: GENERAL AVIATION	D-1
	APPENDIX E: INTERNATIONAL AVIATION SECURITY	E-1
	APPENDIX F: ALTERNATE TVA METHODOLOGIES	F-1
	APPENDIX G: SECURITY SYSTEMS	G-1
	APPENDIX H: FUTURE AIRPORT CONSIDERATIONS	H-1
	APPENDIX I: AREA-SPECIFIC SUMMARY DESIGN CONSIDERATIONS	I-1

TABLES & FIGURES

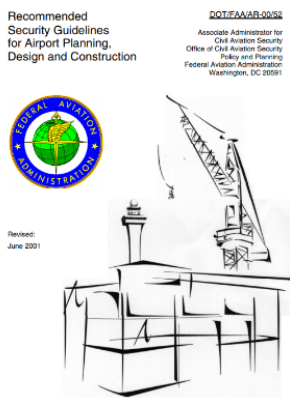
Table 1. Security Areas: Basic Requirements and Descriptions	6
Table 2. Qualitative and Quantitative Risk Analysis Comparison	12
Table 3. Security System Device Coordination	55
Figure 1. Document Links Structure	xiv
Figure 2. Guidebook Section Summary	xv
Figure 3. Security Areas General Description	5

Figure 4. Risk Analysis Matrix – Level of Risk	11
Figure 5. Aviation Terrorist Attacks Timeline: 2011–2017	14
Figure 6. Iterative Protective Design Process	15
Figure 7. Optimal Airport Layout	16
Figure 8. Suboptimal Airport Layout	17
Figure 9. Pressure–Impulse Curve with Element Response	19
Figure 10. San Francisco International Airport, T2 Renovation & Expansion – Landside Bollards	23
Figure 11. Sample Airport Perimeter Fence	27
Figure 12. Sample Camera Resolution Definitions	34
Figure 13. Sample SOC Blocking Diagram	41
Figure 14. Pittsburgh International Airport New Generation Microgrid	63
Figure 15. Manhole Cover Lock	65
Figure 16. Roadway Enclosure	66
Figure 17. Sample Door Hardware Set Schedule	67
Figure 18. Sample Door Hardware Schedule	68
Figure 19. Sample Door Hardware Specification	68
Figure 20. Example of Lock/Key Scheme System	69
Figure 21. Access Panel/Hatch	69
Figure 22. Example of Typical Airport Signage	70
Figure 23. Construction Barricade	73
Figure 24. AOPA Airport Watch Signage	D-2
Figure 25. International Arrivals: Bag Claim after Primary	E-2
Figure 26. International Arrivals Bags First before Primary	E-3
Figure 27. RAMCAP Process Flow Diagram	F-1
Figure 28. ISO 31000 Risk Management Process	F-3
Figure 29. Typical Chain Link Fence Barbed Wire Configurations	G-2
Figure 30. Security Fence with Wildlife Deterrent Fence Skirt	G-3
Figure 31. Single Fixed-Imager Camera	G-8
Figure 32. PTZ Camera Field of View Example	G-9
Figure 33. Multi-Imager Field of View Example	G-9
Figure 34. Panoramic Field of View Sample	G-10
Figure 35. I-Frame vs. P-Frame	G-12
Figure 36. Future Employee Screening Portal	H-2
Figure 37. OSS Concept	H-3
Figure 38. Cargo Facility Diagram	I-14

SUMMARY

This document represents the sixth iteration of guidance for the airport security planning and design community, first issued by the FAA in 1996 and 2001, continued by the TSA in 2006 and 2011, and last published by National Safe Skies Alliance (Safe Skies) in 2017. All iterations have had extensive participation and contributions by federal agencies, industry trade associations, and individual architects, engineers, security consultants, and other subject matter experts. The periodic updates have been driven largely by constant changes in both physical and digital technologies, as well as national and international standards, policies, and operational requirements that reflect the changing aviation threat environment. This latest version will address these continued changes, but also reorganizes the document to provide a more traditional AEC (architectural, engineering, and construction) Industry design approach. As a result, relevant aviation security history, background information, and technical information has been relocated to respective sections in the appendices.

It should be noted that, though this document is required by 49 USC § 44914 (2018), its contents are not government regulations or requirements; it is a compendium of real-world experience and best practices developed by aviation security professionals, providing recommendations for airport security, including specific planning and design concepts that are scalable to airports of any size and complexity.



PARAS ACRONYMS

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

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

AOC	Airport Operations Center
ASP	Airport Security Program
ATDS	Airport Technical Design Standards
ATSP	Airport Tenant Security Program
BoD	Basis of Design
CBP	Customs and Border Protection
CHRC	Criminal History Records Check
DBT	Design Basis Threat
EDS	Explosives Detection System
EOC	Emergency Operations Center
EOD	Explosives Ordinance Disposal
FIS	Federal Inspection Services
GA	General Aviation
LAN	Local Area Network
LEO	Law Enforcement Officer
NCIC	National Crime Information Center
NFPA	National Fire Protection Association
ORAT	Operational Readiness and Acceptance Testing
PBIED	Person-Borne Improvised Explosive Device
PDD	Project Definition Document
PIDS	Perimeter Intrusion Detection System
PSIM	Physical Security Information Management
RTCA	Radio Technical Commission for Aeronautics
SOC	Security Operations Center
STA	Security Threat Assessment

SVA	Security Vulnerability Assessment
TVA	Threat and Vulnerability Assessment
UPS	Uninterruptible Power Supply
VMS	Video Management System
VCIN	Virginia Criminal Information Network
WAN	Wide Area Network

HOW TO USE THIS DOCUMENT

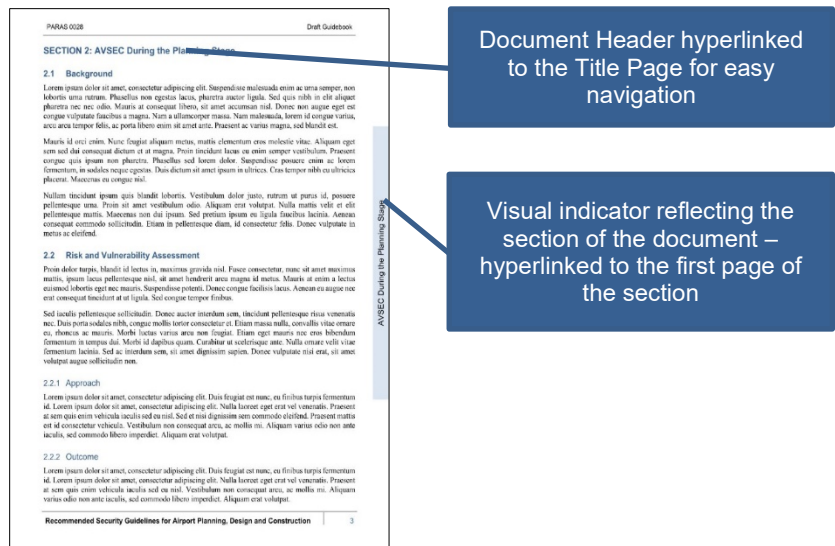
This guidance document has been developed to enable the reader to adhere to the following traditional aviation security design process from concept through final acceptance. When a new airport construction project is identified, the security design process should begin at the initial stages of the project concept. At that time, it is recommended to develop or update the airport Threat and Vulnerability Assessment (TVA), along with a blast assessment, depending on the location and criticality of the project. The outcomes of the TVA and blast assessment will lead into the development of the airport’s security requirements through a Project Definition Document (PDD). Once approved, the PDD is translated into project-specific functional requirements for each of the various elements of the airport’s security systems involved with the project. The systems are then engineered, designed, and coordinated, and then issued for construction. The selected contractor’s first task is to develop shop drawings reflecting the design intent. Once approved, the construction phase begins with equipment installation, testing, and system commissioning, and ends with final acceptance by the owner. The details of this process are included throughout the document.

Where there is a relevant, industry-accepted and publicly available guidance document, this document will reference, summarize, and include a hyperlink to it. However, this document is not intended to repeat or copy information from those documents.

This document has been configured to be utilized both in an electronic PDF viewer and printed hardcopy. When utilized with a PDF viewer, the reader will have the ability to:

- Move to the first page of a section by clicking the sidebar
- Select external hyperlinks from within this document

Figure 1. Document Links Structure

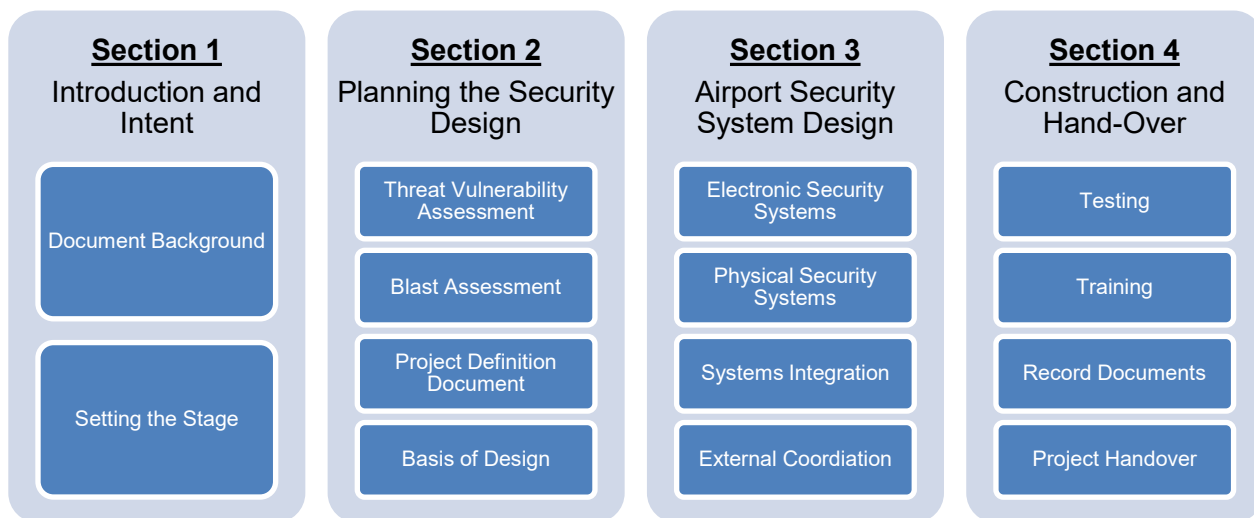


DOCUMENT ORGANIZATION

As this iteration has been organized in a different fashion and structure, a brief description to the document structure and what is contained within each section is provided below. The target audience for each section has not been specifically identified, as this document is intended to provide an overarching guide and approach to security planning, design, and construction for owners, architects, engineers, and contractors.

The guidebook is divided into four primary topic sections, as shown in Figure 2. Appendices are also included to provide greater detail on the history of this guidebook, aviation security regulations, and technical descriptions for the various systems and areas of the airport identified throughout the document.

Figure 2. Guidebook Section Summary



Section 1 introduces the document and provides background regarding regulatory requirements for aviation security and its criticality to protection of the traveling public.

Section 2 focuses on the initial stages of a project where security considerations are critical. It addresses the process of completing a TVA and a blast assessment. The TVA will provide options for mitigating the identified threats to the project, whether operational or physical. The blast assessment will identify the risk to the project location based on explosive charge weight and stand-off distance. The mitigation measures agreed upon will be translated into a PDD, which becomes the minimum baseline security requirements for the project. The PDD is then translated into a Basis of Design (BoD), which provides the technical requirements for the security systems.

Section 3 addresses the design process utilizing the BoD to create design and engineering drawings, and specifications for procurement. In addition, this section provides guidance on coordination and integration needs with external systems that interface with and/or support the security functional needs. A critical element in this section is the development of the systems integration requirements between the security systems and external systems (e.g., access control system controlling baggage shutter induction points). Proper coordination is critical to meeting the requirements of the PDD and ensuring a fully integrated security program.

Section 4 focuses on the process of construction, including developing testing procedures, maintaining security during construction, training recommendations, system handover, and final system acceptance

by an owner. The testing program will need to ensure the new security systems are performing per the requirements identified in the PDD and BoD, along with the manufacturer performance specifications. Training requirements are identified along with the different types of recommended training based on the role of the security operator. And finally, the process of project handover, which includes identifying the documents for project closeout, proper transfer of ownership from construction to operation, and the start of the warranty and maintenance period.

Appendices provide additional technical and design guidance for the various topics covered within the guidance document. They also provide guidance on areas of the airport that may not be applicable to all projects, including US Customs and Border Protection (CBP), general aviation (GA), and cargo facilities.

SECTION 1: INTRODUCTION AND INTENT

1.1 Setting the Stage

Incorporating security requirements and concerns into the planning and design process at the earliest phases of planning and development is critical. Timely consideration of such needs will result in less obtrusive, less costly, and more effective and efficient security systems and measures. Proper planning can also result in reduced labor requirements and consequential reductions in overhead expenses.

However, including security systems and operations in the planning and design of airport construction and redevelopment projects can be a very complex task. The term “security systems” covers a broad range of equipment, technologies, procedures, and operational approaches that require clear and concise guidelines. Any airport planning, design, or construction project is also further challenged by an environment of evolving threats, often accompanied by the implementation of new regulatory requirements and operational updates to counter the changing threat conditions.

Airports tend to be in a constant state of change in terms of their physical layouts, operations, and tenants. Many of the major airports in the United States have exceeded their intended operational lifespan, and therefore significant redevelopment of airport terminals is occurring and will continue in the future. However, the majority of security changes, upgrades, or replacements will be accomplished in existing facilities that are often decades old, with structures designed at a time when the threat profile and the security environment were dramatically different than they are today.

All of these points emphasize that there is not a single, one-size-fits-all solution to the circumstances encountered at each airport when designing and integrating security measures and systems, nor is there a design/build/commission or design/build processes that can be universally applied to all airports.

This guidance document is intended to help mitigate these challenges and ensure that security considerations and requirements are a significant component of the planning and design of airport infrastructure, facilities, and operational improvements. This document contains no legal or regulatory mandates, but the guidance document itself is required by 49 USC § 44914 (2018). The planning and design concepts are current to late 2020.

1.2 Applicability

This document provides options, recommendations, and guidelines, but it is not intended to suggest mandatory measures for any US airport nor a prescriptive approach to aviation security design. The information is provided for consideration by airport operators and planners, as well as consultants, designers, architects, and engineers engaged in renovations and new airport facility planning, design, or construction projects.

Some of the recommendations may have broad application at many airport facilities, while others may apply only to a limited number of airports, facilities, or security situations. Parties involved in airport security development projects are encouraged to review these guidelines for applicable security considerations and coordination, as well as resulting changes to the physical layout and security procedures.

Portions of this document outline procedural aspects of operational processes, extending beyond design and construction concepts. These are included here as a brief tutorial in operational subject matters that may be unfamiliar to the designer/architect. The authors consider it vital that the designer understand the

complexities of such processes and the range of alternatives available to the airport operator—and thus to the designer—before a design can appropriately accommodate space allocation, queuing, equipment, surveillance, power, communications, and other security infrastructure needs. A goal of this document is to facilitate meaningful discussion between designers, airport operators, security experts, and the aircraft operators on ways to meet security requirements in a cost-effective manner.

Although the information provided is primarily of interest to commercial airports regulated under 49 CFR § 1542, some suggestions may be useful for consideration by GA airport operators as well. Refer to Appendix C for additional information on GA security guidelines.

1.3 Considerations

Use of this document at the start of the airport planning and design process helps ensure that security needs are adequately considered. Security features that have been factored into initial facility design and coordinated through all interested stakeholders are more likely to be cost-effective, better integrated, and more operationally useful than those added on to existing structures through late involvement in the design process.

Checklists are located at the conclusion of each section to assist in providing consistent coordination, consideration, and inclusion of security features in an efficient and effective manner. Essential considerations include:

- Access to and between the AOA, SIDA, Secured Area, and Sterile Area, which are defined in 49 CFR § 1542 and in each Airport Security Program (ASP)
- Flow of both passengers and employees from landside to Sterile/Secured Area and back
- Efficient and effective security screening of persons and property entering Sterile Areas, including consideration for queuing space during peak loads
- Separation of secure areas and use of required and recommended signage
- Identification and protection of other vulnerable areas and assets
- Protection of aircraft, people, and property
- Blast and hostile vehicle mitigation measures
- Space and infrastructure for checked baggage inspection systems (CBIS) and devices
- Space and flexibility for advanced passenger screening technologies at the checkpoints
- Accommodation of integrated infrastructure for advanced surveillance, and access controls with biometrics
- Command and control capabilities for improved situational and domain awareness.

Users of these guidelines are reminded that equipment related to physical security, access control, screening, and detection, as well as structural barriers, are fully effective only if supported by similarly effective operational policies and procedures. These include access and ID media systems, challenge procedures, personnel security training and procedures, maintenance training and procedures, as well as constant supervision and vigilance. Appropriate early coordination with airport law enforcement agencies, fire and building code officials, emergency response agencies, operations and maintenance personnel, and other end users and tenants is vital for effective and efficient airport security.

1.4 Changing Security Concerns and Contingency Measures

Airport planners and designers are encouraged to consider the potential impact that changing security threats can have on airport facility design. As an example, during development of this document the Novel Coronavirus (SARS-CoV-2, COVID-19) spread globally and severely impacted the aviation industry. Recovery from the pandemic and the resulting security improvements and modifications will be studied and evaluated after publication of this document, but should be considered for projects moving forward. Planners and designers should consult with airport security coordinators (ASC), airport and aircraft operators, TSA officials, and other relevant stakeholders to ensure that designs facilitate the implementation of new requirements and contingency measures.

Additional contingency plans identified in an airport's ASP and Airport Emergency Plan (AEP) must also be considered. For example, the Gerardo Hernandez Airport Security Act of 2015¹ requires airports to put in place working plans for responding to security incidents, including terrorist attacks, active shooters, and incidents targeting passenger checkpoints. Such plans must include details on evacuation, unified incident command, testing and evaluation of communications, timeframes for law enforcement officer (LEO) response, and joint exercises and training at airports. In addition, the AEP will identify the local emergency response and the types of services to be accommodated, and may require additional or alternative uses of airport facilities during emergency conditions. As a result, all airport contingency plans and actions should be considered during airport construction or refurbishment.

¹ Public Law 114–50 (49 USC 44903): <https://www.congress.gov/114/plaws/publ50/PLAW-114publ50.pdf>

SECTION 2: PLANNING THE SECURITY DESIGN

2.1 Planning for the Design

Planning for security must be an integral part of any design project undertaken at an airport, including physical structures, IT systems, power requirements, among others. General planning, design, construction, and operational requirements of a commercial airport are established and administered by the FAA. The security planning, design, and operations requirements are approved by the TSA. Additional guidance and information is also provided in a series of FAA Advisory Circulars (A/C) for various elements to be considered from initial planning through completion of a project. Ensuring the inclusion of security systems, methods, and procedures within this construction and operational process is a joint responsibility of the airport and the TSA, especially when the construction impacts access to the Sterile and Secured Areas.

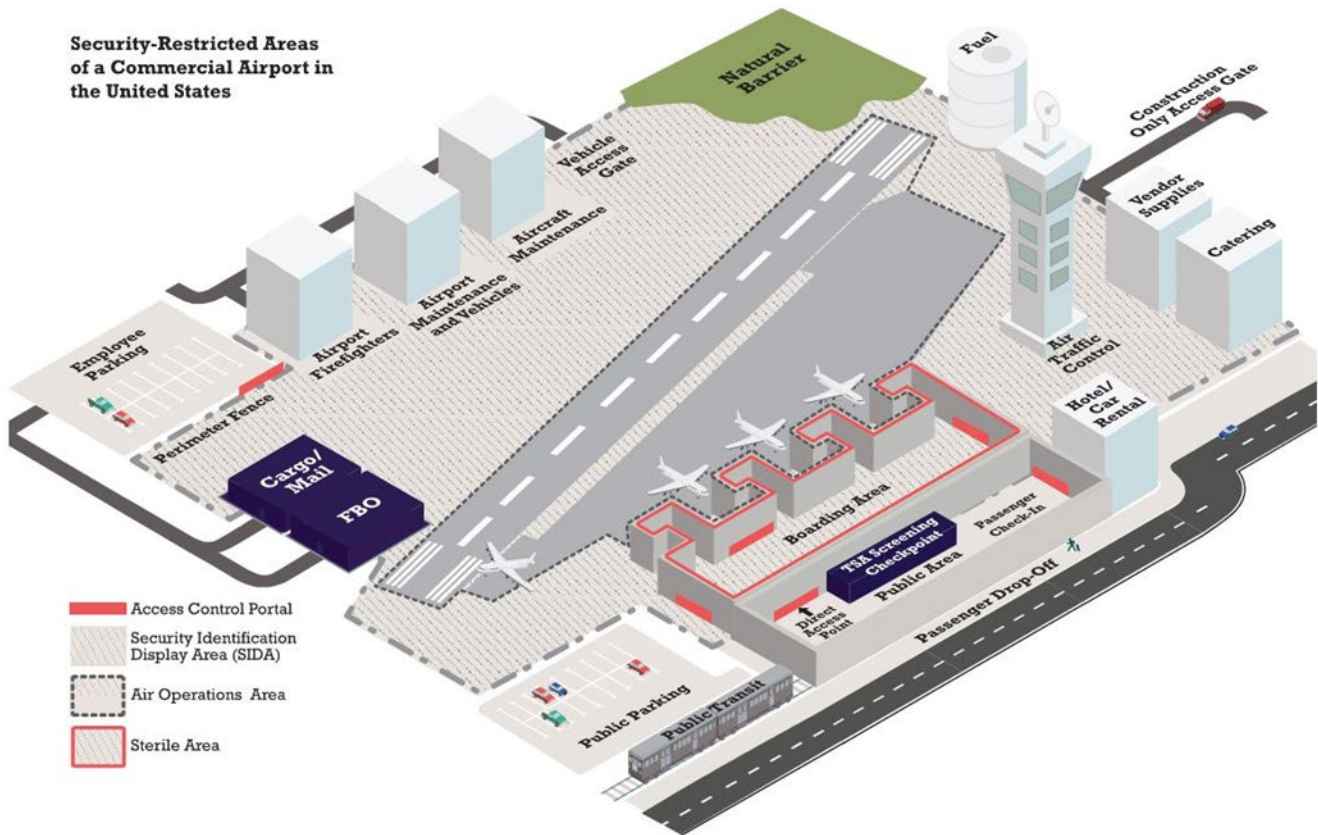
The primary objective of facility protection planning is to ensure both the integrity and continuity of operations, security of assets, and protection of the traveling public. Approaches to physical security should reflect applicable federal, state, and local laws, regulations, and policies to ensure the protection of all persons and assets (including information systems and data).

Once a project has been identified, the airport's planning and design team should consider consulting experts in the field of aviation security. Such expertise is available from several sources, including aviation associations, internal experts, professional consultants, and the TSA. The team should coordinate with the appropriate federal, state, and local security agencies throughout the contracting process, construction, installation, and training. Relevant stakeholders should be provided with all pertinent information, including timelines, status reports, and points of contact, so that adjustments can be made when changes occur throughout the project.

2.1.1 General Security Areas and Boundaries

Several components of airport operations should be considered when planning for the protection of an airport facility. Figure 3 is a generic depiction of the various security-related areas at a typical commercial airport, such as a terminal, aircraft apron, taxiways or runways, and other components that are more comprehensively shown on an FAA-approved Airport Layout Plan (ALP). The ALP is one of the first documents suggested for review; it will show the airport property and the major facilities at an airport.

Figure 3. Security Areas General Description



When planning for facility protection, the following points must be incorporated:

- Any area designated as requiring control for security and/or safety purposes must have identifiable boundaries for that area to be recognized and managed. In some cases, boundaries must meet a regulatory requirement to prevent or deter access to an area. In many instances, boundaries may not be hard physical barriers, such as fences or walls; they might instead be painted lines, lines marked and monitored by electronic signals, grass or pavement edges, natural boundaries such as water or tree lines, or geographic coordinates. The distinctions between different areas must be understood by the design team, such that they are clear on how the physical design of space and structures relates to the physical and virtual boundaries.
- Security Area Basic Requirements: Table 1 provides general comparative descriptions and regulatory requirements (including training, criminal history records checks [CHRC], and ID display) for the three basic airport security areas: Secured Area, SIDA, and AOA, which are defined in 14 CFR § 153.3. Discussions must be held with the local ASC and FSD for further localized definitions at the airport.

Note: Some airports and design professionals use the term Restricted Area. This is a broad generic term, and does not carry a specific definition in US airport security regulations. However, it may be used locally to describe other areas of non-public concern, such as administrative offices, supply rooms, telecommunication rooms, etc.

Refer to Appendix A for definitions of each of these areas and Appendix I for associated considerations.

Table 1. Security Areas: Basic Requirements and Descriptions

	Secured Area	SIDA	AOA	Sterile Area
Regulatory Requirements	<ol style="list-style-type: none"> 1. Access controls meeting 49 CFR § 1542.207 2. Security training 3. Full CHRC and TSA Security Threat Assessment (STA) 4. ID display/ challenge 	<ol style="list-style-type: none"> 1. No access controls required by regulations 2. Security training 3. Full CHRC and TSA STA 4. ID display/ challenge 	<ol style="list-style-type: none"> 1. Basic access controls meeting 49 CFR § 1542 2. Provide security information 3. STA required 	<ol style="list-style-type: none"> 1. Access controls meeting 49 CFR § 1542 2. Controls per ASP 3. CHRC and STA required
Security Level	Highest level of security including access controls, training, CHRC, STA, and ID display/challenge procedures	SIDA relates to ID display and CHRC/STA only.; access controls are determined by requirements of AOA, Sterile, or Secured Area location	Broadest application of security; requirements are not specifically set forth in 49 CFR § 1542 STA required	Sterile Area(s) may be SIDA, depending upon the ASP CHRC and STA required
Relational Description	A Secured Area is always a SIDA, because all three SIDA elements are present: Training, CHRC/STA, and ID display/challenge procedures; the Secured Area goes beyond SIDA by also requiring access controls	SIDA lacks access controls, so a SIDA cannot be a Secured Area	The AOA requires only basic access controls, but sets no specific standards beyond those adopted locally in the ASP	The Sterile Area begins immediately after the screening checkpoint(s) and extends to the boundaries of the Secured Area and/or SIDA, where access controls are required to enter the more secure areas.

2.2 Initial Project Planning

For new construction or extensive renovation, airport facility planners and designers should encourage early formation and involvement of an Airport Security Committee that includes the affected aircraft operators and tenants, fire and building code officials, local FAA, TSA and other federal officials where required based on the project scope and impact, local emergency response personnel, and the airport’s security department. The committee’s role is to assist planners and designers in factoring the appropriate security and safety perspectives into plans and designs, and to accommodate anticipated long-term expansion and regulatory changes where possible. This is captured in the development of a PDD, discussed in Section 2.4 below, where early security-oriented reviews of design plans will identify user requirements of all parties, and can alert project managers to potential integrated security approaches that may be more operationally and economically suitable.

Local security officials, including the FSD responsible for the airport, can also assist planners by providing assessments of the security environment. These assessments should focus on prevalent sources of threat and the history of criminal/violent activities likely to impact airport security and operations, and could include recommended countermeasures. Careful attention must be given to

coordination with the regulatory requirements found in 49 CFR §§ 1540 and 1542, specifically the definition and controls for the various security operational spaces at the airport.

Consideration should also be given to the needs of law enforcement, security, and safety support personnel. Planners and designers are urged to coordinate with local and federal law enforcement and life safety agencies, local emergency response agencies, canine and explosives ordnance disposal (EOD) response elements, and, where relevant, local representatives of CBP. Refer to Appendix E for elements of international aviation security and its impact on US airports.

In addition to planning with various security agencies and reviewing regulatory security documents, advanced planning for the impacts of construction is critical to ensure the continuity of the security systems during construction. This will include addressing the following:

- Temporary security – This may include electronic security systems being taken offline to relocate/transfer primary power sources, relocate an IT/security closet, blocking/removing/relocating a SIDA access portal, construction barricades blocking surveillance cameras, etc. For each potential condition, an alternate security plan should be developed.
- Temporary AOA fence relocation – There may be a period when the AOA fence needs to be removed or repositioned. Considerations may include temporary fencing to meet the standards of the AOA fence, posted security guards if the period of time is short, or constructing a new AOA fence before the existing one is removed. Any active perimeter intrusion detection system (PIDS) may also be impacted. Depending on the fence modifications, either the system will need to temporarily bypass the affected zone or the PIDS will need to be temporarily reconfigured.
- Temporary access points – The construction work area may impact existing access control portals, requiring a new temporary portal to be constructed to provide access between the zones. If the temporary portal is governed by a regulatory requirement, time will need to be allocated to properly test and certify the door before bringing into operation.

Early planning with the airport security department is not only critical for identifying potential project impacts, but also defining security needs and requirements during the early phases of a project.

2.3 Security Workshops

Aviation security is not solely the responsibility of the security department; all credentialed staff have a level of responsibility. As a result, when a security project is in the initial stage of planning, security workshops facilitated by the security group are the key to successful designs and deployments. These workshops should meet regularly, especially at major project submissions to review and provide feedback to the design team.

At a minimum, the following groups should be part of the security workshops and/or solicited for input:

- Design and Construction – Assists in sourcing products and services, developing scopes of work, and cost estimation. Design and Construction may also provide guidance on airport design standards, construction management, and airport installation standards.
- FSD or their local equivalent – Assists in modification of plans and procedures, specifically addressing and providing guidance on regulatory requirements.

- Security Manager/ASC – Assists in system coordination planning, developing scopes of work, feasibility studies, and cost estimation. The ASC is responsible for ensuring the security of the airport is maintained throughout the project, and for updating the ASP as needed when impacts to regulated spaces occurs.
- Risk Management – Provides guidance for modifying areas of the airport depending on the areas of construction or impact to operations, and provides risk evaluation for construction. Specific guidance may be provided when the area of work is in the AOA and evaluation/modification of the Safety Management System is required.
- Fire Department – Assists in applicable codes and provides compliance advice. Depending on the jurisdictional responsibility of the airport, the fire department may also serve as the authority having jurisdiction who will review and approve design plans for code and life safety requirements. Early involvement will assist in addressing code issues and potentially facilitate quicker design reviews.
- Emergency Management/Emergency Planning – Assists in modifying plans and procedures, as well as training and exercise needs. In addition, this group would need to be aware of any demolition work and if material safety data sheets are required for any controlled equipment or installation practices.
- Contracts and Administration – Assists in sourcing products and services, developing scopes of work, and cost estimation. One of the challenges, especially with public agencies, is the requirements for open bid projects versus sole source solutions. This may require developing a sole source justification letter to remain with a specific manufacturer/model of a security component.
- Dispatch/Communications/Operations Center – Assists in system coordination planning. This group can also assist with modifications to security software applications or updates to the software as needed to support new security devices.
- Engineering – Assists in identifying relevant codes and standards, developing scopes of work, feasibility studies, and cost estimation. Engineering may also assist with locating existing infrastructure needed to support projects, and providing power requirements and fire alarm interfaces, where required by code.
- IT – Assists in system coordination planning, developing scopes of work, feasibility studies, and cost estimation. Depending on the operation of the airport, IT may provide network support for security systems, and address any potential upcoming IT system upgrades that may impact the project.
- Law Enforcement – Assists in modifying plans and procedures, assessing effectiveness of mitigation options, and providing guidance on local and regional threats.
- Operations (landside, airside, terminal) – Assists in modifying areas of the airport impacted by construction. Operations may be required to inform airlines, vendors, and tenants of the areas of impact and potential modifications.
- Badging/Credentialing – Assists in modifying plans and procedures, assessing effectiveness of mitigation options, and compliance. They will also assist contractors with the credentialing process or alternative access measures.
- Air Carrier – Assists in defining operations, including access control needs that are important to supporting operations. When providing financial support to the project, their input and support is critical.

2.4 Project Definition Document (PDD)

The outcome of the security workshops should be captured in a PDD, which is a statement of the purpose and goals of an airport security system or upgrade program, as determined by the facility's stakeholders and users. The process of creating a PDD is iterative, and must balance operational needs and regulatory requirements with available technology, design challenges, and cost effectiveness. When developing the PDD, the following questions should be addressed:

- What does the project involve? Examples include an update of existing infrastructure, a move or expansion into new facilities, operational reorganization, and new interfaces with airport departments and government agencies.
- Why is this project happening? Examples include system integration, physical expansion, growth forecasts, outdated technology, new regulatory requirements, inadequate or failing infrastructure, and administrative restructuring.
- Who are the users and stakeholders, both internal and external to the organization? What are their operational goals? What information do they require?
- What infrastructure exists?
- What threats and vulnerabilities exist?
- Which new technologies will best serve the different priorities and interactions among user groups?
- What human factors need to be accommodated? Examples include ergonomics, lighting and noise levels, sight lines, dealing with multiple technologies and/or multiple events, and staffing/training criteria.
- What is the realistic budget and how was it established? Are there additional related costs, such as those for staffing and long-term training, operations, and maintenance?
- What are the required levels of protection for the development of the blast assessment?
- What critical infrastructure and associated threats need to be considered?

One of the goals of a PDD is to identify operational requirements in sufficient detail to form the BoD. The PDD provides operational guidance on how the systems will be used and is invaluable in determining which systems are needed and the benefits they will provide. The PDD should help drive the selection and design of technologies because, all too often, technologies are selected and implemented without a thorough understanding of the organization's needs, which can result in underperforming systems that are never used.

The PDD is not a static document; it evolves as the organization evolves, as new threats emerge, as new tools become available during design and construction, and to provide for expansion.

2.5 Threat and Vulnerability Assessment (TVA)

Every airport operator, owner, or sponsor and their respective departments have varying risks that influence how they achieve their objectives and goals, thereby affecting airport planning and design, as well as operational effectiveness. It is important to measure and prioritize risks so that the airport and airport authority can respond to any given situation appropriately, efficiently, and effectively, to ensure minimal operational loss.

2.5.1 Reference and Guidance Documents

For additional guidance on TVAs and risk assessments, refer to:

- [PARAS 0016 – Airport Security Vulnerability Assessments](#)²
- [ASIS International Risk Assessment ANSI/ASIS/RIMS RA.1-2015](#)³
- [ISO 31000:2018 Risk Management Guidelines](#)⁴

2.5.2 Value of Threat and Vulnerability Assessments

Conducting frequent TVAs is critical because of the ever-changing environment that airport planners encounter. Comprehensive TVAs offer an organized and systematic approach to assessing risks and evaluating the safety and security mitigation measures being utilized. This approach provides the analytical framework for risk management.

A TVA should identify key assets that need to be protected and determine how critical each asset is to the business of the airport and its operation. Past focus has emphasized a segmented view of assessing risk, whether it be physical security, cyber security, or operational aspects. But all these aspects need to be intertwined to ensure proper design and planning of countermeasures that help the airport achieve its objectives and establish a flexible framework that can be scaled and improved as the airport operation matures.

Comprehensive TVAs involve not only physical, informational, cyber, and operational security knowledge, but how these aspects affect each individual operational unit. This requires a complete understanding of airport operations and thorough review of every threat and vulnerability to determine appropriate, coordinated mitigation measures.

PARAS 0016 – Airport Security Vulnerability Assessments is a vital resource for airport design and planning, as it presents an effective methodology. However, airport planners and designers should also consider other processes that can enhance the methodology presented in the document.

2.5.3 Quantitative and Qualitative

There are two main methods of risk analysis: quantitative and qualitative. Quantitative analysis involves interpreting numbers from data and estimates. Qualitative analysis involves interpreting interviews, words, and images. ISO 31000:2018 and other standards such as the ASIS/RIMS/ANSI Risk Assessment standard determine that risk can be assessed by using a quantitative, computational approach; a qualitative, subjective approach; or a combination of the two.

Quantitative analysis is always a component of qualitative analysis, even when the quantitative analysis is indirect. Quantitative analysis is based upon numeric data. The idea of quantitative analysis is that if one can examine a problem from enough points of view and measure or estimate each of those elements, one can understand enough about it to make valid conclusions. Qualitative analysis involves the description of the data's characteristics, attributes, features, or value (cost of replacement/cost of impact to operations), and the estimating of those values in general terms (low, medium, high, etc.) A risk analysis matrix for both quantitative and qualitative analysis is shown in Figure 4 below.

² For download: https://www.sskies.org/images/uploads/subpage/PARAS_0016.SVAGuidebook_Final_.pdf

³ For purchase: <https://store.asisonline.org/risk-assessment-standard-softcover.html>

⁴ For purchase: <https://webstore.ansi.org/Standards/ISO/ISO310002018>

Figure 4. Risk Analysis Matrix – Level of Risk

Likelihood	Consequences				
	Insignificant (1) No injuries/ minimal financial loss	Minor (2) First aid treatment/ medium financial loss	Moderate (3) Medical treatment / high financial loss	Major (4) Hospitable / large financial loss	Catastrophic (5) Death / massive financial loss
Almost Certain (5) Often occurs/once a week	5 Moderate	10 High	15 High	20 Catastrophic	25 Catastrophic
Likely (4) Could easily happen/once a month	4 Moderate	8 Moderate	12 High	16 Catastrophic	20 Catastrophic
Possible (3) Could happen/once a year	3 Low	6 Moderate	9 Moderate	12 High	15 High
Unlikely (2) Has not happened by could/once every 10 years	2 Low	4 Moderate	6 Moderate	8 Moderate	10 High
Rare (1) Conceivable but only on extreme circumstances/ one every 100 years	1 Low	2 Low	3 Low	4 Moderate	5 Moderate

Risk Outcome
Low
Moderate
Significant
High

As PARAS 0016 *Airport Security Vulnerability Assessments* points out, each approach has its merits. Airport designers and planners need to decide which is the best method to determine risk and an understandable cost benefit analysis for their specific circumstances. Table 2 provides a comparison of the two approaches, as well as a third, hybrid approach.⁵

⁵ Will Ozier, “Chapter 3-1-1 Risk Analysis and Assessment,” *Handbook of Information Security Management*, <http://www.blacksheepnetworks.com/security/info/misc/handbook/223-228.html#Heading1>

Table 2. Qualitative and Quantitative Risk Analysis Comparison

Quantitative Assessment	Qualitative Assessment	Hybrid
Pros		
Assessment and results are based substantially on independently objective processes and metrics. Thus, meaningful statistical analysis is supported.	Calculations are simple and readily understood and executed.	Qualitative analysis is often conducted from a basis of quantitative data. The most effective reports are the result of both quantitative and qualitative approaches.
The value of information is expressed in monetary terms. With supporting rationale, it is better understood. Thus, the basis for expected loss is better understood.	Not necessary to determine quantitative threat frequency & impact data.	Quantitative data can sample very large quantities of data, whereas qualitative analysis usually focuses on a small data field. The use of quantitative data helps assure that the small data sampled for the qualitative analysis is truly representative, relevant to the issues, and less biased by personal prejudices.
A credible basis for cost/benefit assessment of risk mitigation measures is provided. Thus, security budget decision-making is supported.	Not necessary to estimate the cost of recommended risk mitigation measures and calculate cost/benefit.	
Cons		
Calculations are complex. If they are not understood or effectively explained, management may mistrust the results.	Risk assessment and results are essentially subjective in both process and metrics.	
A substantial amount of information about the target and its environment must be gathered.	No effort is made to develop an objective monetary basis for the value of targeted assets.	
Qualitative analysis can be prone to significant flaws unless the analysis is based on critical thinking processes.	No basis is provided for cost/benefit analysis of risk mitigation measures. Only subjective indication of a problem.	

2.5.4 Methodologies & Approaches

The Security Vulnerability Assessment (SVA) methodology recommended for airports in PARAS 0016 is based on reviews of methodologies used in other sectors, assessments of stakeholder feedback, and identification of key success factors. The methodology borrows from existing processes and adapts them to facilitate identification of:

- Relevant airport assets and functions of concern
- Relevant reference threats for airports
- Quantitative and qualitative risk identification and rating processes that are valid, flexible, and easy to implement

Sections 4.5 and 4.6 of PARAS 0016 describe steps to identify threat likelihood and vulnerability that aim to streamline both the risk identification process and the prioritization of assets and hazards. Aside from the airport focus and recommendations regarding threat likelihood and vulnerability, the suggested methodology is like those used in other critical infrastructure sectors and relies on the equation:

$$\text{Risk} = \text{Consequence} \times \text{Probability} \times \text{Vulnerability}$$

Identifying a security vulnerability and risk assessment methodology for airports requires discussion of scope and scale. Most government-derived methodologies, such as the DHS Threat and Hazard Identification and Risk Assessment (THIRA) Guide are asset-, facility-, and/or process-focused, and much more tactical in nature.

Other industry-derived consensus standards indicate the need for a hybrid methodology for airports that focuses primarily at the asset/facility/process level but gives some consideration to the community approach prescribed in the THIRA Guide. Various industry standards focusing on the asset/facility/process level provide valid models from which an airport-specific risk assessment model can be formed.

PARAS0016 details an SVA approach that would provide a standard baseline for airports. However, it would be prudent to conduct a thorough review of other methodologies considering the specific airport, its operations, and the particular objectives of the owner, project, and anticipated output usage of the TVA. Additional methodologies are identified in Appendix F.

2.6 Blast Assessment

A blast assessment can be performed concurrently with a TVA that includes a qualified blast engineer, or after the TVA to bring more definition to an identified vulnerability and quantify the expected consequence of an explosive event. The TVA will serve to establish the explosive threats, which are then used by the engineer to determine the ‘loading’ imposed on the building or non-building structure (e.g., overpass, utility tunnel). Additionally, the TVA will identify the “asset value” of each structure which will further define the expected performance of the structural element.

It is expected that the TVA would identify the explosive modality (e.g., vehicle-borne, person-borne, mail); however, it more than likely would not identify the specific information needed to fully develop design basis threat (DBT) scenarios for the assessment. It would also not identify the specific performance of architectural and structural components that would lead to the detailed identification of vulnerabilities followed by development of mitigation solutions and costs.

2.6.1 Reference and Guidance Documents

For additional guidance on blast design and mitigation, refer to [PARAS 0014 – Blast Mitigation Strategies](#).⁶

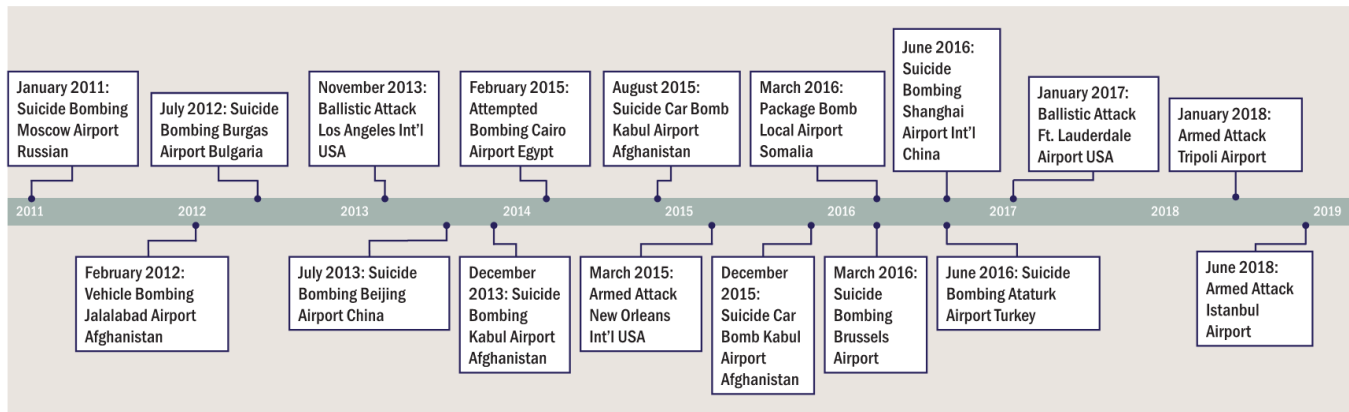
2.6.2 Historic Events

In light of recent bombing attacks at both international and domestic airports, the need to implement protective design measures has become a priority for mass transit facilities. Airports are uniquely

⁶ For download: https://www.sskies.org/images/uploads/subpage/PARAS_0014.BlastMitigationStrategies.FinalGuidebook.pdf

vulnerable due to the far reaching impact of an attack, especially for those that are major hubs for international travel. As shown in Figure 5, there have been numerous explosive and armed attacks at airports and other mass transit facilities throughout the world in recent years. While a number of attacks are within high risk regions, the frequency and spread of events is alarming, and has brought awareness and a call to action by the aviation industry to increase security.

Figure 5. Aviation Terrorist Attacks Timeline: 2011–2017



2.6.3 Design Challenges

History shows the need to enhance airport design to provide a safer environment for employees and visitors, however, incorporating blast mitigation measures presents challenges. Fear of the costs associated with blast hardening often causes decision makers to overlook implementation of protective measures altogether. Additionally, lack of clarity and direction leaves owners and design teams confused about how to provide a baseline level of protection. One goal of this document is to—in conjunction with PARAS 0014—clearly show how cost-effective measures can be implemented to increase protection.

2.6.4 Assessment Process

The blast assessment process is often iterative, as shown in Figure 6, and requires continued collaboration between design team disciplines, stakeholders, and contractors. To provide cost-effective solutions for blast mitigation, beginning the blast assessment at the early stages of the project is crucial. Changes to the design throughout the design process often have an impact on the overall risk and vulnerability. For instance, providing blast hardening reduces the vulnerability to damage associated with a blast event. Similarly, relocating critical operations away from public spaces reduces the risk of an explosive attack. This iterative process and close coordination between the team allows for a design that balances hardening for blast and other protective measures.

Figure 6. Iterative Protective Design Process



Differences in the process are common for new construction versus evaluation of existing airports. New construction allows for the design team to tweak aspects of the design to reduce vulnerability against an explosive event, while existing construction has less flexibility. Especially when assessing an existing building, it is essential to provide the blast engineer with as much detail of the existing conditions as possible—detailed structural, architectural, site drawings as well as in place security measures—while also keeping them informed about expected modifications and the design vision. In many cases, new terminal construction or a new addition is planned on an existing site, which presents its own set of challenges. Close coordination and early team integration limits the challenges and can result in a more economic design.

2.6.4.1 At-Risk Spaces

As part of the TVA, spaces with highest risk for an explosive event should be identified. An important aspect of the blast assessment is to focus efforts on protecting the high-risk spaces, as it is not beneficial or cost effective to implement protective measures throughout the terminal. For instance, because an unscreened privately-owned vehicle will not have access to the AOA, and all passengers undergo TSA security before entering the Sterile Area, consideration of an explosive threat within these spaces is not necessary.

Areas of high risk are airport dependent. However, the following are commonly considered high risk for an explosive threat:

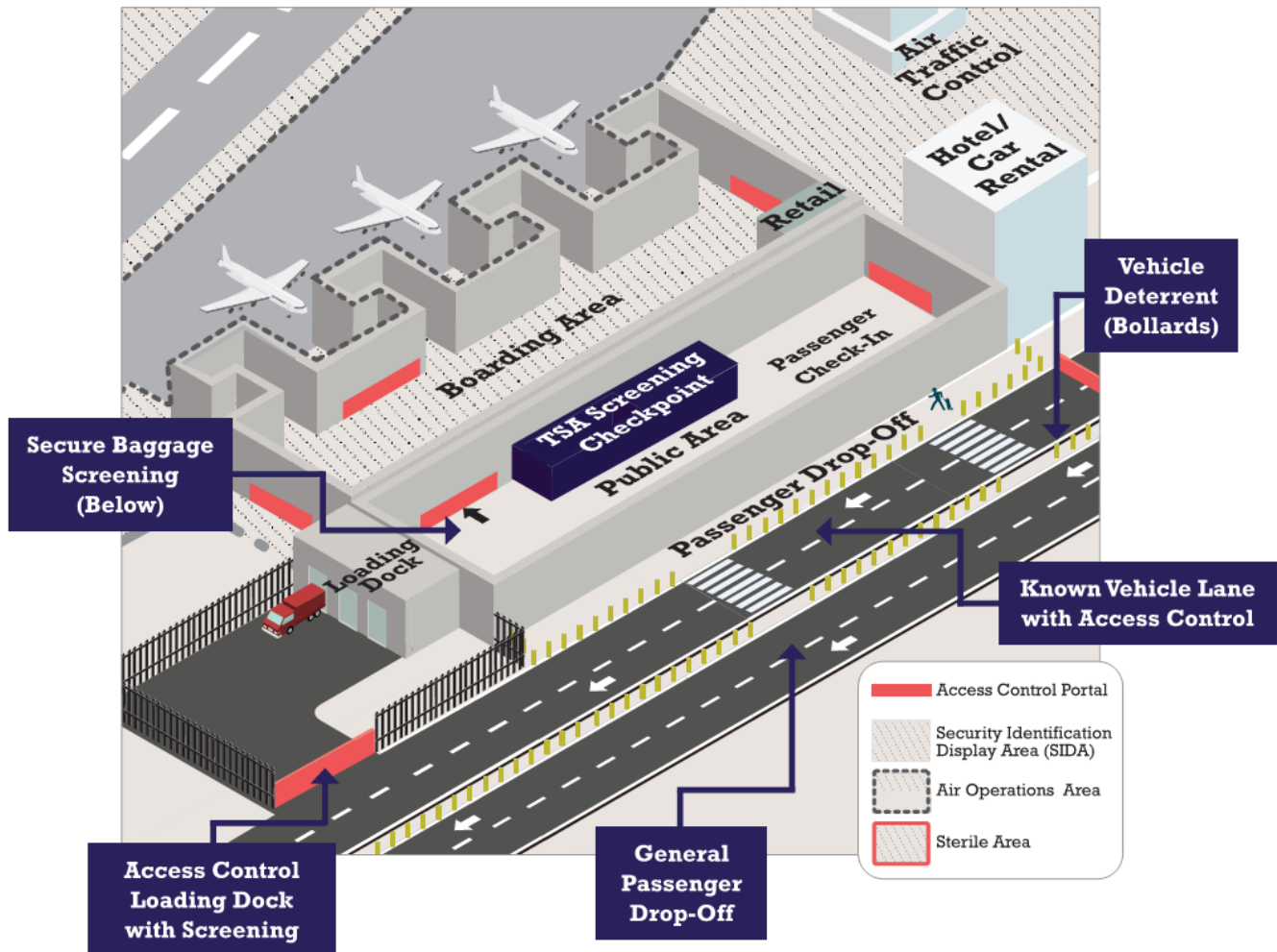
- Terminal drop-off/pick-up areas that allow privately owned vehicles to idle near terminal entrances/exits without suspicion.
- Crowded spaces at entrances/exits exterior to the terminal and within the terminal prior to screening.
- Public areas and functional areas within the terminal that handle unscreened packages, such as the baggage screening area and the loading dock.

Focusing efforts on these and other high-risk areas provides much greater benefit to protection of employees, visitors, and airport assets.

Schematic concept diagrams highlighting optimal versus suboptimal airport space layout are provided in Figures 7 and 8. The following features are highlighted in the optimal space planning scheme:

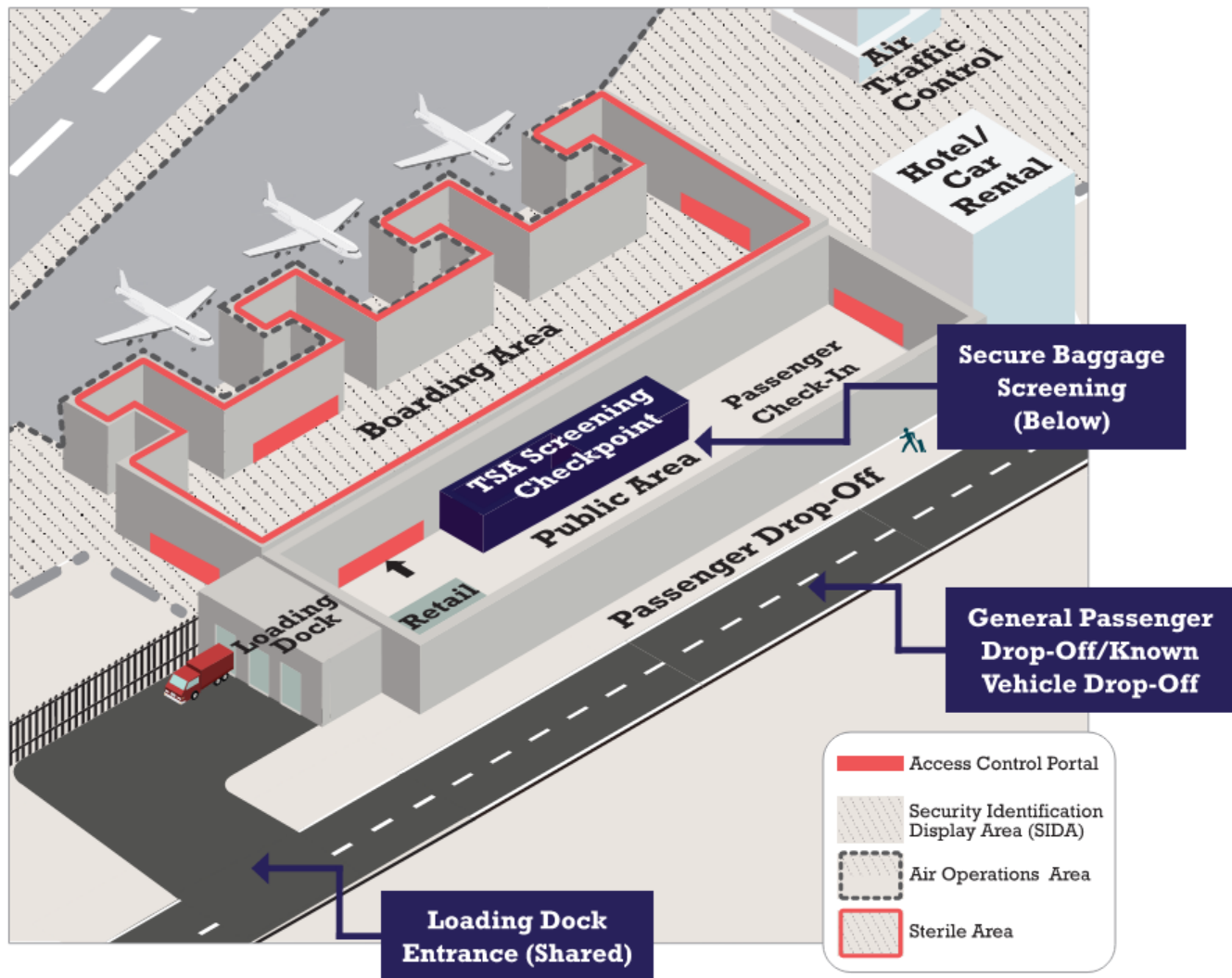
- Allowing only screened/known vehicles to access roadways closer to the terminal frontage and providing access control at those areas; general passenger drop-off/pick-up would be located at a roadway further from the terminal frontage
- Providing a separate entrance to loading dock areas with access control measures
- Locating retail and restaurants within the Sterile Area to limit crowding within unscreened areas
- Locating secure baggage screening areas away from crowded spaces

Figure 7. Optimal Airport Layout



Section 2: Planning the Security Design

Figure 8. Suboptimal Airport Layout



2.6.4.2 Design Basis Threat Scenarios

Although explosive threats are commonly IEDs, due to availability of material, industry standard for consideration of an explosive threat assumes a weight of explosive in terms of TNT equivalency at specific standoff distance (the distance between a target and the explosive detonation). IEDs can be person-borne (PBIED) or vehicle-borne (VBIED), considering an explosive weight that can reasonably be held on a person (suitcase or package) or within a vehicle, respectively.

Results of the TVA define the DBT (an explosive weight, standoff scenario, or a combination of both), as these are often dependent on the airport and take into consideration target attractiveness (density and operations) as well as the additional security measures in place, such as access control, video surveillance, or police presence. Common DBT scenarios are as follows:

- PBIED within interior public spaces
- VBIED at uncontrolled public roadways
- Large VBIED at nearest designated parking area

In addition to explosive threats, a risk analysis should identify if additional threats need be mitigated, such as an active shooter (individual or coordinated) or vehicle ramming. The armed, ballistic attack, and vehicle ramming scenarios are best mitigated through operational measures and the placement of protective elements rather than structural and façade hardening. These measures will be addressed in subsequent sections.

2.6.4.3 Performance Objectives

Given the nature of a blast event, it is often not feasible to design the structure or façade to remain undamaged when subjected to blast loading. As such, performance criteria for the building components typically allows for some level of damage. The intent is to provide effective protective design measures that minimize mass casualties due to an explosion by achieving the following:

- Limited structural collapse
- Maintained building envelope
- Minimized flying debris hazards

These principles are expanded on in PARAS 0014. Typically, performance criteria for building components is established considering the allowable level of damage, and is often based on the overall targeted level of protection for the airport. The TVA should identify the level of protection for the airport in question based on the criticality of the airport and associated risk.

Often, the performance criteria or level of accepted damage may differ between types of building components (primary versus secondary structural elements), different DBTs (a more likely close-in PBIED versus a less likely large VBIED at a further distance), and the consequence of failure and/or expected risk. Tailoring the allowable damage in this way results in a more cost-effective design.

2.6.4.4 Assessment Results

Knowing the DBT scenarios and targeted performance of the structure under those scenarios, the engineer can utilize different approaches to understand the performance and determine mitigation solutions to improve the structure's performance. Two common approaches to blast assessment of the structural and architectural components are classified as follows:

- Performance-Based Approach – Evaluating the performance of structural and architectural components in terms of the expected level of damage considering a specified DBT (known threat size and detonation location)
- Capacity-Based Approach – Determining the maximum threat size given a known threat location that allows the structural or architectural component to maintain an acceptable level of damage. Alternatively, determine the minimum standoff given a known threat size to achieve the acceptable level of damage.

This concept can be better explained using an example DBT scenario that considers a VBIED at the terminal ticketing drop-off roadway. In this example, the primary concern is the failure of the exterior terminal façade, which would result in hazardous fragments and blast overpressures entering the interior public space and causing injury to building occupants.

Using the performance-based approach, upon gathering sufficient information, a computer/virtual model is created of the façade system, in which a known VBIED charge weight is placed at the roadway and the

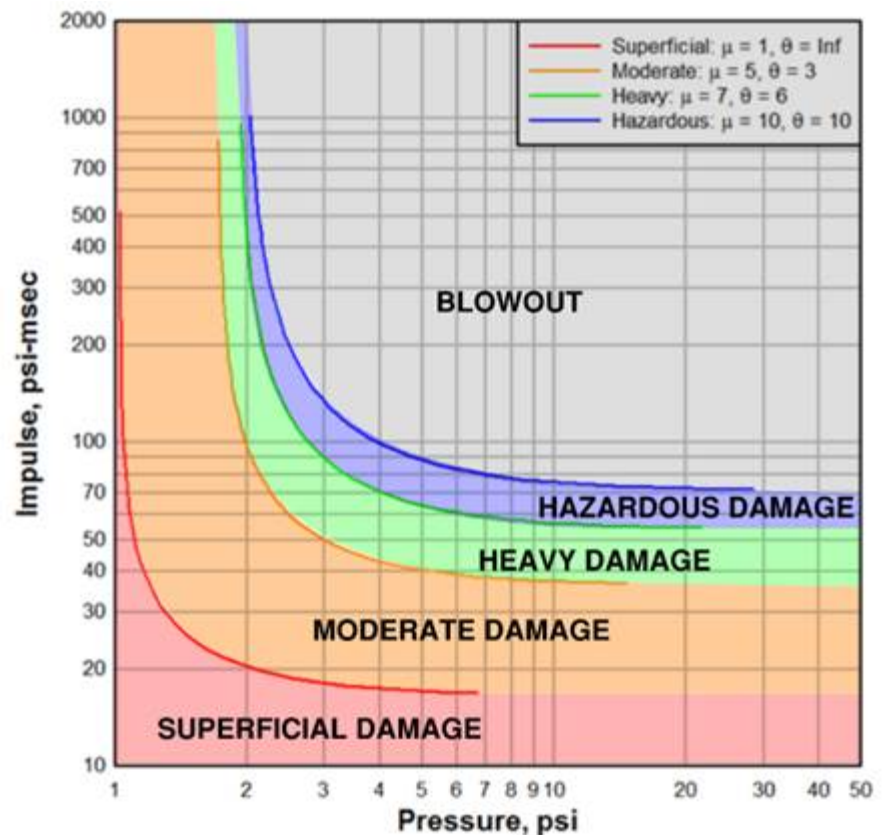
resulting blast loading is applied to each structural and façade component. From this analysis, the expected damage is obtained. Where the expected damage is in excess of the allowable limit, elements are upgraded until the targeted performance is reached.

Alternately, using a capacity-based approach, the engineer can determine the maximum charge weight at the specified roadway by starting at a low charge and working up to the point before the façade fails. Or, if given a specified charge weight, the engineer can move the VBIED forward to the minimum standoff point before the façade fails. Note that analysis methods for evaluating components for blast loading are expanded on in PARAS 0014. Additionally, PARAS 0014 provides common upgrades to structural and architectural components that can be used to increase performance.

The most effective approach is a combination of the two approaches, using cost-effective upgrades to increase the level of performance against a reasonable explosive threat. Starting with the performance-based approach in our example, the engineer evaluates the system under the specified charge weight and results show that the performance is unacceptable. Upgrading the system to meet the desired performance is not feasible from a cost standpoint, but some level of upgrade can somewhat improve the performance. Upon understanding the upgrade that can be implemented, in collaboration with the team, the engineer can make adjustments to the site or security measures to either reduce the expected credible threat size or increase the standoff distance to the terminal façade. This achieves the desired performance with a cost-effective solution.

Pressure–impulse (P–I) curves illustrate the relationship between the standoff distance and/or charge weight and structural/façade performance. P–I curves are created by plotting the response, usually in terms of element ductility and rotation for a specific damage state, associated with a number of P–I combinations, as shown in Figure 9. The curve makes it simple to understand what pressure–impulse combination would allow for the desired level of damage or, alternatively, understand the damage associated with a specific P–I. P–I curves may also be applied to a 3D building model to understand locations where upgrades may be necessary and where loading is not significant enough to result in undesirable damage.

Figure 9. Pressure–Impulse Curve with Element Response



Source: KPFF Consulting Engineers

2.6.5 Best Practices and Industry Trends

The appearance of a robust security presence, both operational and fixed, serves as a visual deterrence to a potential aggressor. The introduction of structural design best practices into the standard design process also provides a considerable improvement in a structure's resistance and resilience to extreme loading, whether it be by manufactured or natural hazards.

Physical hardening best practices include measures such as compact steel sections, ductile detailing, mitigation of brittle modes of failure, designing structural connections to develop the capacity of the element they support, and use of deterrent systems, such as non-rated vehicle barriers, to enforce increased standoff and reduce the likelihood of an event.

Operational measures can also help minimize the potential threat and reduce the overall risk associated with one or multiple hazards simultaneously. These can include roving police K-9 units, and police vehicles at terminal drive-up/drop-off and pick-up curbside areas.

Providing some level of protection has become standard in the industry. The trend at newly constructed and renovated airports includes the following design aspects to increase protection:

- Shelter-in-place/duck-and-cover measures or areas of refuge provide building occupants with increased safety in the event of an explosive attack, active shooter, or vehicle ramming.
- Laminated glass in all exterior glazing systems limits hazardous debris associated with an explosive threat or active shooter.
- Segregating space between the Sterile and public areas through planning or with a full height partition limits the ability of an aggressor to target areas beyond the TSA checkpoint. Utilizing laminated glass for a glazed partition will limit hazardous debris; ballistic or blast-rated glazing would further increase protection. Additionally, providing a means to close off the Sterile Area using glazed doors or a roll-up door is common.
- Though not addressed in detail in this document (reference PARAS 0014), loading docks present a vulnerability to a VBIED. Providing access control at loading docks limits this vulnerability.
- Create an inner and outer roadway at locations nearest the terminal to limit access at the inner roadway to known vehicles only; unknown vehicles will be restricted to the outer roadway. This increases the potential standoff for a VBIED and limits accessibility for a vehicle ramming.

Additional hardening options are presented in PARAS 0014, such as encasing steel columns in concrete or concrete columns in steel jackets. PARAS 0014 also expands on utilizing a balanced design approach for window systems to ensure the glazing fails prior to the mullions and supporting structure.

2.7 Hostile Vehicle Assessment

In recent history, attacks involving intentional vehicle ramming of soft-target, densely populated outdoor areas have become increasingly common. Areas most vulnerable to a vehicle ramming incident, both intentional and accidental, are those along terminal drive-up drop-off, populated sidewalks, terminal entrances/exits, and crowded interior ticketing and baggage claim areas that are enclosed by large expanses of transparent curtain wall facades and within direct approach of a vehicle. Where the threat is intentional, the building itself is not generally a target, just densely populated areas within. The target attractiveness is often dictated by the number of people gathered in the area, as the aggressor is interested in causing the maximum number of casualties.

The purpose of a hostile vehicle assessment is to evaluate the vulnerability of an existing or proposed site layout to possible vehicle approach scenarios and determine mitigation measures to reduce those vulnerabilities. Vulnerabilities lie where vehicles can reach high speeds through a direct (straight) path of travel to impact densely populated areas. These can be mitigated by providing obstacles to limit a direct approach (e.g., curved roadways, lane dividers, curbs) or implementing rated or non-rated barriers to stop or deter a vehicle.

2.7.1 Vehicle Vector Analysis

A vehicle vector analysis is performed to understand the vulnerability associated with a vehicle impact by determining the speed at which a vehicle can impact a target considering a specific path of travel. Industry-accepted guidance for a vehicle vector analysis can be found in [UFC 4-022-02 Selection and Application of Vehicle Barriers](#).⁷

Factors such as vehicle weight, initial speed, travel distance, turn radius, and roadway slope are considered in determining the expected impact velocity of the vehicle. Additional considerations such as curb placement and roadway friction can also be included for more accurate predictions. The results of the vehicle impact analysis are typically presented as risk in terms of the kinetic energy at impact given a vehicle weight and impact velocity.

2.7.2 Site Design

The most effective approach for mitigating a hostile vehicle threat is reconfiguring the site to prevent a direct path of travel to densely populated areas. Where the site design cannot accommodate redirecting roadways or relocating public vehicle access away from a vulnerable area, vehicle barriers should be utilized as a best practice.

2.7.3 Crash Ratings

There are a number of industry standards for determining the vehicle-impact capacity of crash-rated bollards. Two of the most common standards are the Department of State (DoS)/Department of Defense (DoD) K-ratings and ASTM International Designations. Crash ratings are dependent on the vehicle type: Small Passenger Cars (2,430 lb), Pickup Trucks (5,070 lb), or Medium Trucks (15,000 lb). Of these vehicle sizes, a pickup truck is the most commonly used for design of barriers domestically, including for government and airport facilities, since their target attractiveness and asset value warrants a larger vehicle.

Section 4.1.5 of PARAS 0014 provides further explanation of crash ratings for vehicle barriers considering both the K-rating and ASTM designations.

2.7.3.1 Barrier Selection and Existing Conditions

Barrier selection is highly dependent on an airport's risk posture, existing conditions, vehicle and pedestrian traffic flow, and aesthetic considerations. Selection of a rated barrier will also depend on the design basis vehicle size as noted in Section 2.7.3, and calculated impact speed. When considering barrier placement, it is recommended that, at a minimum, barriers be located at public entrances and exits. Other locations include exterior areas of congregation (e.g., transit stops, shuttle bus pick-ups), and large expanses of transparent curtain wall façade that are positioned in a direct approach of a

⁷ For download: https://www.wbdg.org/FFC/DOD/UFC/ufc_4_022_02_2009_c1.pdf

vehicle. In general, the clear distance between barriers should not exceed four feet, but this may vary based on the system rating.

Site design considerations should provide for sufficient space between the curb and barriers to ensure passengers can exit their vehicle and easily navigate around them with luggage. This will reduce traffic congestion by allowing for quicker passenger drop-off. Additionally, site surveys and as-built drawings should be reviewed during the design process to locate underground utilities and determine foundation constraints.

At elevated roadways, it will be necessary to attach barriers to existing structural elements, which will require an assessment of element's capacity to sustain the imparted reactions upon vehicle impact. In this instance, a structural engineer should be consulted to perform a rigorous analysis to ensure the stability of the elevated roadway is not compromised and that the barrier will perform as intended.

2.7.3.2 Visual Deterrents and Engineered Barriers

The appearance of a robust security presence, both operational and fixed, serves as a powerful deterrence to a potential aggressor. This can be accomplished by means of police vehicles at populated curbside areas, as well as the placement of engineered barriers or other vehicle deterrents. Means to deter vehicles without using rated barriers include boulders, planters, benches, or non-rated bollards. While these solutions are not technically rated, they do have some capacity to stop or slow a vehicle. Additionally, engineered solutions such as jersey barriers and water-filled barriers have a modest capacity to stop a vehicle, but are more commonly used to defend against an accidental vehicle ramming.

2.7.3.3 Current Trends

Implementation of vehicle barriers has become the standard of practice at both small and large airports. Most airports with new or newly renovated terminals have implemented some level of hostile vehicle mitigation, ranging from robust crash-rated bollards along the entire terminal frontage to concrete benches, planters, or other landscape elements surrounding terminal entrances/exits. Installation of barriers should be considered in consultation with qualified design professionals, which should always include civil, architectural, structural engineers, and most importantly a physical security/protective design engineer with the expertise to perform a vehicle vector analysis.

In addition to barriers, airports are also realigning roadways to reduce approach vehicle velocity as well as segregating known vehicle (e.g., airport shuttle buses) lanes from unknown vehicle (e.g., privately owned vehicles, taxis, etc.) lanes, with the latter located further from the terminal. Additionally, passenger pick-up, and at times drop-off, are being relocated to parking garages across the terminal roadway or at remote transit centers where passengers must take airport shuttles to the terminal. It is apparent that the future of transporting passengers to and from an airport terminal will continue to evolve with security as a priority. However, passenger experience must also be considered.

Figure 10. San Francisco International Airport, T2 Renovation & Expansion – Landside Bollards

Source: Designed by Gensler; Photography by Nic Lehoux

2.8 Basis of Design (BoD)

Upon completion of the PDD, which is used to complete the TVA and blast assessment, the recommended mitigation measures are documented into the BoD. The BoD is the formal bridge between the PDD and the design process, establishing the technical, operational and space requirements necessary to meet the PDD goals.

To be clear, the BoD is not a design; it serves as a means for the airport owner-operator and Architectural/Engineering Department to define the parameters of the design by examining various ways to meet functional requirements. Each option should be described in sufficient detail, along with its advantages and disadvantages, plus estimated costs, to determine the best options. A typical BoD will include the following elements:

- General facility description, including backup documentation
- Interagency coordination requirements and communications
- Facility location or possible alternatives
- Space requirements and descriptions
- Regulatory and code requirements

- Requirements for redundancy, reliability, and recovery
- High level description of the physical security systems (bollards, structural reinforcements, barriers, etc.)
- High level descriptions of engineered systems (mechanical, electrical, fire protection, etc.)
- High level descriptions of security functions and systems

The BoD will generally not include descriptions of operations and policies or procedures, though it must continue to be informed by these. When the BoD has been completed, the design team will have a documented baseline of expectations and requirements from which to develop, design, and refine the facility and its supporting elements to produce documents suitable for construction.

2.8.1 Protection of Sensitive Security Design Information

In the process of developing the security design, SSI will be created as defined by 49 CFR § 1542.5. Example of SSI as part of a security design would include the TVA, blast assessment, and field of view of the surveillance cameras. The author of these documents has a duty to protect the information, both in electronic and physical (paper) forms.

As a general guidance, the following minimum level of protection should be applied to developed project information. Specific requirements should be reviewed in advance with the Project Information Officer to ensure proper compliance.

TSA has developed an SSI Best Practices Guide which provide guidance on the proper handling of SSI created documents. The full version of this document can be obtained at [TSA SSI Best Practices Guide](#).⁸

Also see Safe Skies' [PARAS 0008 Findings and Practices in Sharing Sensitive Information](#).⁹

2.9 Planning the Security Design Checklist

The following summary checklist encompasses the initial stages of planning the security design for a construction project.

- Establish Airport Security Committee
 - Identify airport stakeholders
 - Identify design team stakeholders
- Develop PDD to be flexible; technology and regulations change
- Develop TVA with mitigation options
- Develop Blast Assessment with mitigation options
- Planning and design considerations:
 - Physical security-level boundaries
 - Prevent items being passed through/over physical boundaries
 - Deter public access to nonpublic areas

⁸ For download: https://www.tsa.gov/sites/default/files/ssi_best_practices_guide_for_non-dhs_employees.pdf

⁹ For download: https://www.sskies.org/images/uploads/subpage/PARAS_0008.SharingSensitiveInfo.FinalReport.pdf

- Obtain copies of all relevant security guidance documents
 - Airport Authority Design and Construction Guidelines
 - Regulatory agency guidance documents (TSA, CBP)
 - Applicable codes and standards (International Building Code, National Fire Protection Association [NFPA], local building code)
- Develop BoD for the physical and electronic security systems
- Develop airport security zoning plans per Table 1
- Consider contingency and security operational plans during construction
- Coordinate access points; minimize crossing security boundaries
- Limit concealment areas/structures
 - Minimize concealment areas
 - Minimize and lock accessible spaces
- Different operational pathways for:
 - Passengers and airport personnel
 - Tenants/concessions
 - Emergency response routes
 - Delivery routes
 - Security response; police escorts
- Adhere to SSI handling procedures
 - Obtain or develop the project SSI handling procedures
 - Obtain or develop a non-disclosure agreement to be signed by all parties who will need access to SSI documents
 - Develop and provide a training program for handling of SSI documents
 - Audit SSI handling procedures during the lifespan of the project

SECTION 3: AIRPORT SECURITY SYSTEM DESIGN

3.1 Physical Security Systems

To define and adequately protect the AOA, SIDA, and other restricted areas from unauthorized access, it is important to consider boundary measures such as fencing, walls, or other physical barriers, electronic boundaries (e.g., sensor lines and alarms), and natural barriers (e.g., bodies of water) in the planning and design process. Access points for personnel and vehicles through the boundary lines, such as gates, doors, guard stations, and electronically controlled or monitored portals, should also be considered. Additional security measures that would enhance these boundaries and access points are clear zones on both sides of fences, security lighting, locks, video surveillance systems (VSS), and signage.

The selection of an appropriate security boundary design is not only affected by the cost of equipment, installation, and maintenance, but also by the more important aspects of effectiveness and functionality. The highest consideration in an effective boundary measure is its ability to prevent unauthorized penetration. Thus, any access points through a boundary line should not only be able to prevent access but differentiate between an authorized and an unauthorized user. At an airport, access through boundary lines can be frequent and should be quick to prevent unacceptable delays. In addition, if a boundary access point is not user-friendly, it may be abused, disregarded, or subverted, and thus pose a security risk.

Regardless of boundary location or type, the number of access points should be minimized for both security and cost efficiency. Proper planning and design can often create fewer access points that are more functional and maintainable, which will benefit the airport in the long run.

3.1.1 Natural Barriers

Natural barriers can be used to form part of the physical security system to deter and delay access to the restricted areas. Natural barriers may consist of large bodies of water or earthen materials (mountain, berms, etc). Typically, natural barriers are supplemented with electronic detection solutions.

When considering whether any natural barrier is an appropriate boundary, the airport should incorporate the findings of the TVA. The natural barrier may need to be complemented with other types of boundary protection. Special attention should be given to areas where significant bodies of water are used as public recreational or fishing areas near the airport boundary.

3.1.2 Physical Barriers

Physical barriers can be used to deter and delay the access of unauthorized persons into nonpublic areas. These are usually permanent and designed to be obvious visual and physical barriers. They also serve to meet safety requirements in many cases. Where possible, security fencing or other physical barriers should be aligned with security area boundaries.

3.1.2.1 Fence

Fences provide a physical and visual deterrent, and define the space between public and restricted-access areas. Fences may be different materials, heights, and levels of protection based on the mitigation recommendations of the TVA.

The fence also provides a mounting location for signage to define the rules and ownership of the space on the secure side of the fence. The location of the signs, language, and size should be defined by the airport based on local codes and legal requirements.

3.1.2.2 Gates

Gates are often required to move authorized personnel and vehicles from the public side to the secure side of the physical barrier. The configuration of the gate should align with the level of protection of the adjacent physical barrier (e.g., fence, natural barrier).

3.1.2.3 Buildings

Buildings and other fixed structures may be used as a part of the physical barrier, and can be incorporated into a fence line if access control or other measures to restrict unauthorized passage through the buildings or structures are taken at all points of access.

Whether access points are located on the airside or landside boundaries, or through the middle of such buildings, may depend on the nature of the business being conducted inside and the level of continuous access required by personnel. Building design should ensure that fire escapes and maintenance access ladders do not provide an unobstructed path from the public side to airside.

3.1.2.4 Walls

Walls are one of the most common types of physical barriers. Various types of walls are used for interior and exterior security boundary separation. Walls also play an important part as visual barriers and deterrents.

When interior walls are to be used as security barriers, consideration should be made to their type, construction material, and height. When possible, security walls should be full height, reaching beyond suspended ceilings. Interior walls may be used as part of the security boundary, with appropriate attention paid to maintaining the integrity of the boundary and the level of access control to a degree at least equal to that of the rest of the boundary.

While typically not as economical as chain-link fencing, the use of exterior walls as physical barriers and security boundaries may be necessary. Walls provide less visibility of storage or Secured Areas, and can be matched to the surrounding architecture and buildings. In addition, some types of wall are less climbable than security fencing or other barriers that offer handholds.

Walls should not have hand or foot holds that can be used for climbing. The tops of walls should be narrow to prevent perching, and should have barbed wire or other deterrent materials. Exterior walls over 12 feet may not require barbed wire protection. Blast mitigation walls are not necessarily good security fences, although appropriate design can aid in incorporating features of both, spreading the cost over more than one budget.

Figure 11. Sample Airport Perimeter Fence



As in the case of interior walls, exterior building walls may also be used as part of the security boundary, as long as the integrity of the restricted area is maintained to at least the level maintained elsewhere along the boundary.

Not all exterior walls are designed to mitigate a breach due to the physical construction of the wall and structure. For example, brick walls perform best in compression and provide limited protection from a horizontal attack. Appropriate wall types and configurations need to be selected that can mitigate a failure with a perpendicular attack approach.

3.1.3 Reference and Guidance Documents

ASTM International provides guidance on the testing protocols for physical security systems in [*Standard Test Method for Crash Testing of Vehicle Security Barriers*](#).¹⁰ This document is a “for-purchase” reference standard.

Also see Safe Skies’ [PARAS 0015 – Guidance for Airport Perimeter Security](#).¹¹

3.1.4 Design Checklist

- Define the perimeter between the landside and airside
- Define natural barriers and assess the level of protection and penetration
- Define physical barriers to supplement and enhance the natural barriers
- Confirm regulatory and legal requirements for signage along the physical barrier

Refer to Appendix G for a summary of various physical security systems for consideration.

3.2 Electronic Security Systems

Electronic security systems include various types of technology and devices, which—either separately or integrated—combine to enhance the overall facility’s security. The most common of these technologies are access control systems, PIDS, and VSS.

3.2.1 Access Control Systems (ACS)

An access control system (ACS) generally consists of database-based software that is operated in conjunction with field devices (e.g., card readers, locking mechanisms, sensors) to control access through portals or sensors to detect activity on security boundary lines. The regulatory purpose of an ACS is to deny access to unauthorized persons and to control the passage of staff into Secured and Sterile Areas as outlined in 49 CFR § 1542 and the airport’s ASP. While these systems are only required for TSA-regulated airports, various types of ACS are implemented in airports of all sizes, and are often multi-purposed for access control in non-regulated airport areas.

Airport ACS are designed for managing and controlling access of credentialed individuals through controlled portals. These systems are not designed to control the access of passengers or aircraft crew members to the Sterile Area.

¹⁰ For purchase: <https://www.astm.org/Standards/F2656.htm>

¹¹ For download: https://www.sskies.org/images/uploads/subpage/PARAS_0015.AirportPerimeterSecurity.FinalReport.pdf

ACS are normally considered in two parts. The first is the vetting, approval, and credential issuance process; the second is a physical ACS that uses the resulting credential to provide or deny access. Any subsequent changes in credential status (active, invalidated, etc.) and/or access privileges must be communicated between the credentialing component and the physical component in a timely and secure manner.

For a complete detailed discussion on airport security ACS uses, technologies, and integrated/associated technologies, refer to the 2019 RTCA DO-230J document, *Standards for Airport Security Access Control Systems*. This document was developed in conjunction with TSA and industry representatives and conveys best practices for developing cost-effective access control systems that meet the needs of all stakeholders.

3.2.1.1 Regulatory Requirements Overview

The regulatory requirements are specified in 49 CFR § 1542. However, airport staff ACS are also the subject of a number of security directives that prescribe special requirements. For security reasons, these special requirements are not described in this document.

From an operational perspective, each airport's ACS and procedures are detailed in their ASP. This information is designated SSI and only shared on a "need to know" basis.

Note that airports exclusively serving GA are not currently required by regulation to have ACS, although their deployment is considered an industry best practice. See Appendix D of this document for additional information related to GA.

3.2.1.2 Performance Criteria

Airport access control systems should be high availability systems operating 24/7/365. System availability should meet or exceed 99.99 percent; performance requirements should be based on risk level.

3.2.1.3 Selectivity

Distinct security zone criteria are defined under current regulations for airports' Sterile Area, Secured Area, SIDA, and AOA; their specific locations and boundaries are detailed in each airport's ASP. The access zones/levels within the ACS at an individual airport may directly correlate with the boundaries of the security zones or may be often be defined in more detail. For instance, from an access control and physical layout standpoint, there may be more than one SIDA/Secured Area, or only certain portions/portals of the SIDA/Secured Area where designated individuals are allowed access. The ACS design, both physically and procedurally, should allow for increased flexibility in controlling different areas, as well as the ability to mitigate risks by limiting when and where persons on an individual or group basis can obtain access.

3.2.1.4 Credentialing

A standard ACS can use physical access media or other non-physical credentials (such as a PIN number) to gain access. In an airport environment, access media is most commonly a physical card/badge, which often serves a dual purpose as an identification credential. In TSA-regulated commercial airports, the combined access media/ID credential design is stipulated by the airport's ASP, and the credentialing process is regulated. Any airport ACS implementation should account for current and/or future credentialing needs.

3.2.1.5 Access Monitoring

An ACS enables an automated process for allowing authorized individuals access to specific security areas and denying access to unauthorized individuals. Generally, this is achieved by use of a credential presented to an electronic card reader at a portal or other entry point. Infrequently used entry points (e.g., roof hatches, equipment closets, etc.) may be monitored by conventional means (e.g., padlocks) but still may have alarm monitoring.

For portals monitored by electronic card readers and other devices, the ACS verifies whether the owner of the credential is entitled to enter, and either unlocks a door or shunts an alarm to allow passage, or denies passage and provides an alert of this denial locally at the door and/or remotely at a command center or Security Operations Center (SOC) where staff can monitor alarms and dispatch appropriate response personnel to the scene.

The use of a centralized access control and monitoring system allows for real-time and/or historical tracking of an individual's access, alarm response tracking, and provides a means for changing access authorization from a central location. When combined with a VSS, particularly if integrated for automatic video display of alarm areas, security effectiveness can be increased and personnel requirements can be reduced.

The same credential can also be used at staffed security portals (vehicle gates, etc.), non-security general-use portals (back of house, administrative, non-public areas, etc.), and can also incorporate a PIN and/or biometric as an additional authentication factor.

3.2.1.6 ACS Integration with Other Systems

Centralized ACS have the potential to integrate with (or operate in conjunction with) various other airport systems to enhance operational efficiency and security. These systems include:

- ID/Badging/Credentialing Systems – Integration or database-sharing with ACS minimizes data entry and provides for added alarm response features such as ID/badge photo pop-up upon valid/invalid use.
- VSS – Improves alarm assessment/resolution (automated or manually), supplements access verification (general view or comparison of face view to ID photo), and can assist in verification/documenting unauthorized access (piggybacking, etc.) Refer to Section 3.2.3.
- PIDS – Can be integrated to feed alarms into a single central ACS interface for management/response tracking. Refer to Section 3.2.2.
- Vehicle Gates, Portals, and other Physical Barrier Systems – Integration with ACS can result in more efficient throughput and user interface through single-action or remote operation, as well as maximize monitoring capability for barrier/portal function status and/or intrusion and error alarms. Refer to Section 3.2.1.8 Special Security Device Consideration.
- Duress Alarms – Duress alarms can be installed at various locations throughout an airport, including checkpoints, dispatch offices, CBP areas, and ticket counters. Location and installation of these devices is airport- and operational model-dependent. These devices are usually linked to an ACS to provide a common annunciation point.
- Baggage Handling Explosives Detection Systems (EDS), EOD, and Explosives Trace Detection (ETD) Support – Some airports have chosen to install access control and monitoring devices in baggage handling EDS, EOD, and ETD areas to secure the areas and to prevent theft and

interference with equipment. This decision should be based on local conditions and operational practices.

- Screening Checkpoints – Passenger screening checkpoints present some unique challenges for access control:
 1. The checkpoint and access route via the checkpoint need to be secured when it is not in use. This typically requires doors or rollup mesh screens that may be locked from one side or both, depending on the airport configuration. The doors should be controlled and monitored by the ACS. Reduced checkpoint lighting during periods of inactivity may impact surveillance camera performance.
 2. Second is the requirement to validate credentials of Federal Air Marshals, law enforcement officers, and flight crew who bypass screening because they are carrying weapons. Similar considerations apply to members of the Known Crew Member program.
- Exit Lanes – Some exit lane breach control technologies may be integrated with ACS to prevent unauthorized re-entry into the terminal while allowing for maintenance, law enforcement patrols, and other authorized personnel to enter the terminal as needed.

3.2.1.7 ACS Support Requirements

ACS at airports typically have three major support requirements for effective and reliable system operation: power, communications, and HVAC. When possible, the ACS should always be powered by emergency and/or Uninterruptible Power Supply (UPS) or battery backup power for continued operation during outages or incidents.

Communications pathways and technologies should consider redundancy (including physically diverse pathways), reliability under various use and environmental conditions, and cybersecurity.

HVAC ACS considerations should include provisions for operations during the typical environmental extremes for the location (temperature, humidity, sunlight, air flow), as well as for the impacts of ACS and related communication/power equipment heating and humidity on the location in which the equipment is installed.

3.2.1.8 Special Security Device Considerations

Some security devices that may be integrated with ACS have special requirements.

- Anti-Tailgating Devices/Systems – Anti-tailgating strategies may employ specialized systems and equipment to prevent multiple entries into a security area based on a single credential. These systems and equipment include turnstiles, card readers, mantraps, air locks, and various sensors and surveillance technologies (guards, VSS, video analytics, etc.) These may be used at the perimeter, airfield, external facilities, and other security-related areas (security equipment rooms, data centers, bonded/sensitive/restricted areas, etc.)
- ADA Equipment/Requirements – Airports are required to be compliant with the Americans with Disabilities Act of 1990 (ADA). This may require additional equipment and increased clearances at portals. In addition, some states and cities have additional requirements over and above those specified in the federal ADA regulations.

- Fire Door and Emergency Exit Devices – In general, fire detection and alarm systems can be integrated with ACS. Features often include the use of crash bars on fire exit doors linked to the ACS to detect unauthorized operation. During an emergency, these doors may be accessed from public or Sterile Areas directly to Secured Areas and AOA. During normal use, these doors are usually equipped with credential readers that may be used for authorized access by staff.
- Elevators – Elevators should not allow direct access from public to Sterile and Secured Areas, to minimize unauthorized access. However, this may not be possible under some circumstances, and dual-use elevator are not uncommon. In the event of dual-use, access to the Secured and Sterile Areas need to be under the control of the ACS (to include control of call buttons and/or floor buttons), wherever practical. If elevators are used with ACS or on security boundaries, airport operators should consider occupancy detection and internal video surveillance, so that an elevator cannot be boarded at a public floor and then brought down to a restricted floor without warning or positive controls.
- Roof/Access Hatches – When access control is required on a roof or access hatch, challenges may exist in meeting automatic lock and unlock requirements due to limitations on electrified hardware available for a hatch-type portal and/or fire/egress requirements. In many cases, true access control through a roof/access hatch may not be achievable due to both code and configuration of the hatch. Typically, only ACS alarm shunt and user tracking is implemented with manual locking/egress hardware.
- Legacy System Integration – Except in completely greenfield sites, there will usually be some form of legacy access control system, which may need to be interfaced to a new ACS.

3.2.1.9 ACS and Biometrics

Perhaps the most dominant trend in airport access control is the use of biometrics, which may become mandatory in the future. The capabilities of biometric technologies have improved significantly in the last few years, and many airports have already adopted fingerprint-based systems at personnel portals and vehicle gates. Fingerprint-based systems are also used for the credentialing process to enhance ID authentication of the badge holder during background clearance and badge issuance activities.

Alternate biometric technologies such as iris scan, facial recognition, and hand geometry have also considerably improved, but some tend to be slower at high-intensity portals. Nonetheless, they may be appropriate for higher security controls and, in recent applications, support a “touch-free” security portal control system. TSA is also investigating the possible use of biometrics to validate certain categories of passengers; for example, using facial recognition for boarding passes, or touchless fingerprint for high-speed verification.

Industry experts suggest that, although requiring biometric upgrades is likely to occur, the most practical approach would be to implement them during the next scheduled upgrades at each airport in its regular system life cycle. This reflects the fact that all commercial airports already have a regulatory-compliant system in place; some are very new while others are now reaching the end of their operational life cycles. The planners/designers of brand new facilities will need to maintain a level of flexibility and expandability to account for new technologies and/or regulatory requirements in the next series of life cycles for all security-related systems, including IT, fiber distribution, terminal expansion, and future outlying facilities.

Refer to Appendix G for a summary of various ACS technologies for consideration.

3.2.2 Perimeter Intrusion Detection Systems (PIDS)

PIDS technologies are continuing to mature and become more effectively integrated into airport security programs for monitoring and alarm identification. The following should be considered when designing or implementing PIDS:

- Due to the wide variations among airport perimeters, and uncertainties regarding measures that may become required by regulation, it is important that PIDS designs be flexible and adaptable.
- Ground-based radar improvements include the use of multiple frequencies for better target discrimination, and small, solid-state components for “staring” radars, which are less costly than scanning systems, and are suitable for detection at modest ranges. The trend to integrating video surveillance sensors and radars will increase in proportion to the availability of reliable, cost-effective radars.
- Recent advances in economical, eye-safe, high powered, near-infrared diodes for commercial vehicle systems (e.g., autonomous driving and anti-collision functions) will make lidar units increasingly attractive for beam and scanning PIDS applications.
- Integrating multiple sensors, and fusing sensor data with a geophysical map and/or engineering drawing overlays, will continue to evolve and to improve graphical presentations in the SOC.
- More use will be made of wireless connectivity to access sensor data in areas where main power is not available, and to coordinate response actions at event sites.

Refer to Appendix G for a summary of various PIDS technologies for consideration.

3.2.3 Video Surveillance Systems (VSS)

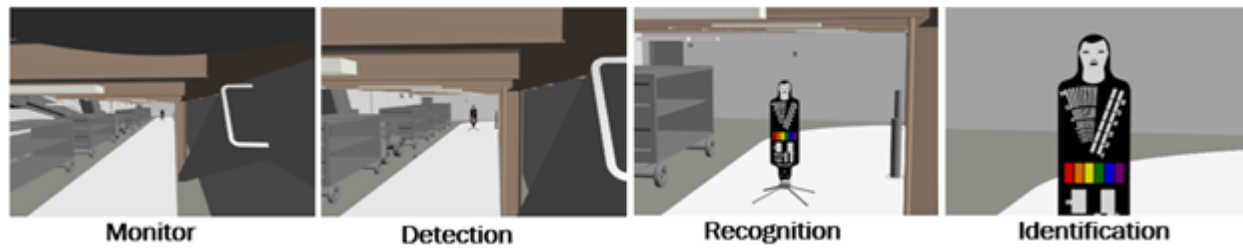
VSS are a critical and key technology when utilized as part of an integrated airport security program. Cameras are used to view activity, support alarm response, and review activity/alarm events over a period of time. Camera technologies are continually evolving with higher pixel counts, number of integrated lenses, and analytic capabilities. Consideration and selection of the type of cameras should be based on the goals identified in the PDD.

The PDD should define the performance objectives and functional requirements of the surveillance system. It should address the question, “Why am I looking at this and what is the objective of this view?” This will assist in developing the intent of the cameras utilizing a common project reference requirement for the view. Typical resolution definitions identify the object size on a monitor along with the pixels per foot (ppf) required at the target, depending on the camera’s functional purpose. These purposes include the terms defined below and illustrated in Figure 12.

- Monitoring – The camera enables viewing of the number, direction, and speed of movement of people across a wide area, providing their presence is known to the operator. The object shall be not less than 5% of the screen height and no less than 5 ppf.
- Detection – The camera enables the operator to reliably and easily determine whether any target, such as a person, is present. The object shall be not less than 10% of the screen height and no less than 15 ppf.
- Recognition – The camera enables the operator to obtain recognition of an individual. The object shall be not less than 50% of the screen height and no less than 60 ppf.

- Identification – The camera enables identification of an individual beyond reasonable doubt. The object shall be not less than 120% of the screen height and no less than 120 ppf.

Figure 12. Sample Camera Resolution Definitions



The Identification level has traditionally been defined as the ability to identify a person in a manner that would be admissible in a court of law. The original definition included viewing the entire person in the image; identification was not based on just the face of the person but included the overall person and clothing. For this definition, 100 ppf is adequate. The definition of Identification has begun to evolve in recent years and is now being used by many manufacturers as being able to identify a person based on facial features alone. Based on this revised definition, industry leaders note that 120 ppf is a viable metric, with 150 ppf to be applied to video with challenging conditions. Challenging environmental conditions include factors such as insufficient lighting, or people, objects, and vehicles moving at high speed.

By taking this design approach, the type and mounting location of the camera will be selected based on the functional requirements identified in the PDD to achieve the “why” and “what” of the camera view.

Refer to Appendix F for a summary of various video surveillance technologies for consideration.

3.2.3.1 Video Surveillance Functional Requirements

Functional requirements provide performance criteria for surveillance cameras. These are typically developed as part of the PDD to provide the design team with the flexibility to adjust the number and locations of cameras in order to meet operational needs.

FUNCTIONAL REQUIREMENTS FOR FIXED CAMERAS

When selecting applications for fixed cameras, the functional requirement of each camera should be clearly defined and include the length of the field of view, as there are limited adjustments for the camera beyond the field of view. An example of a functional requirement where a fixed camera could be deployed would be, “Provide dedicated recognition level coverage of SIDA/Regulatory portal entry and exit points with 30 fps live view and 15 fps for recorded/alarm view.” Design compliance for this functional requirement would require one dedicated fixed camera on each side of the door and positioned to provide recognition-level ppf while supporting the fps requirements.

FUNCTIONAL REQUIREMENTS FOR PAN-TILT-ZOOM (PTZ) CAMERAS

When selecting applications for PTZ cameras, the functional requirement of each camera should be clearly defined due to the narrowing field of view when moved/zoomed. An example of a functional requirement where a PTZ camera could be deployed would be, “Provide supporting recognition level coverage of SIDA/Regulatory portal entry and exit points with 30 fps live view and 15 fps for recorded/alarm view. Camera shall automatically pan/tilt/zoom under alarm conditions on the SIDA/Regulatory portal. Multiple SIDA/Regulatory portals can be monitored by this camera.” Design compliance for this functional requirement would allow a PTZ camera mounted between multiple areas

of interest, and when an alarm event occurs, the camera zooms to the level of recognition ppf while supporting the fps requirements.

FUNCTIONAL REQUIREMENTS FOR MULTI-IMAGER CAMERAS

When selecting applications for multi-imager cameras, the functional requirement of each camera, specifically the lenses, should be clearly defined as the intended views. An example of a functional requirement where a multi-imager camera could be deployed would be, “Provide 180-degree view of a specific area with a look-down view under the camera to provide complete situational awareness of the specific area at 30 fps live view and 15 fps for recorded/alarm view.” Design compliance for this functional requirement would require one dedicated multi-imager camera positioned to view the specific area and provide recognition-level ppf while supporting the fps requirements.

FUNCTIONAL REQUIREMENTS FOR FIXED PANORAMIC IMAGER CAMERAS

Although there are challenges with panoramic cameras, there are potential applications for these cameras in an airport environment. An example of a functional requirement where a panoramic camera could be deployed would be, “Provide general surveillance of the ticket queue area to support situational awareness of the specific area at 30 fps live view and 15 fps for recorded view.” Design compliance for this functional requirement would require one dedicated panoramic camera to view the specific area.

3.2.3.2 Video Surveillance Camera Compression Standards

Although not specifically critical to the selection of the camera for the functional requirement, consideration should be given to understanding the different camera compression standards and the impact to the quality and management of the video.

Refer to Appendix G for a summary of various video surveillance camera compression standards for consideration.

3.2.3.3 Video Communication

IP surveillance cameras are reliant on the data network to provide communication between the camera and Video Management System (VMS) for viewing, recording, and management of the video streams. There are a number of key design factors that need to be considered in the design of the data network, including bandwidth requirements, which should be reviewed with the network systems engineer.

What should be considered and discussed is the data transmission protocol (Unicast or Multicast) used in the network architecture. Unicast and multicast transmissions are two methods in which video is commonly streamed over a network, from the camera to its destination. Each video transmission method comes with advantages and disadvantages.

In a Unicast streaming configuration, the VMS provides a unique media stream based on each workstation request per camera. This transmission ensures that all network packets are delivered to the requesting VMS workstation. For example, if two users are attempting to view a specific camera, in a Unicast configuration, the camera will transmit two identical video streams to the different users, while a third stream is transmitted automatically to the recording solution. The result is a bandwidth load calculation for three identical video streams. This limited example does not pose a significant increase in bandwidth, but what needs to be considered is an emergency situation where multiple users need to access the same camera for situational awareness of the incident. The result could be multiple departments attempting to access the camera, resulting in significant bandwidth increase and exceeding the number of streams the camera can provide. Most cameras can support up to eight unique streams. When this number is exceeded, the ninth stream request would just see a blank screen.

In a Multicast streaming configuration, the VMS requests one unique media stream and the network replicates the video stream to multiple requesting workstations. This is a more effective scheme for multiple clients viewing the same video stream. Multicast configuration does not ensure that all clients will get all the packets in the case of network disruption, but with high network resiliency this is not an issue. In a Multicast configuration, the camera will transmit one live view stream and one recording view stream. The live view can be requested by an unlimited number of user workstations with no limitation on the number of camera streams nor increase in the network bandwidth needs. This configuration eliminates the need to limit user access during an emergency operation with multiple users accessing the same camera. In general, Multicast network configurations are recommended for VSS transmission.

3.2.3.4 Video Image Security and Controls

WATERMARKING AND ENCRYPTION

Recorded video is utilized for multiple applications, including operational analysis, prosecution, and risk mitigation. Considering this, it is critical to ensure the integrity of the image and verify that the video has not been altered when exported from the native VMS recording solution. This is accomplished by adding watermarking and encryption to the video.

A digital watermark is a customizable marker that is covertly embedded in the image data by the VMS on each frame of the video. Exported video streams are typically embedded with the video stream watermark information, the number of current frame bytes, time of video recording, Media Access Control (MAC) address, and serial number of the recording device. The VMS application that encrypts the video is required to play the exported video and verify the integrity of the video stream. The media playing side decodes the code stream data packet and compares the embedded watermark information with the original watermark information. In this way, the security and integrity of the media stream are checked. The method of watermark comparison varies by manufacturer to ensure the integrity of the video but is validated frame by frame. If the media stream is invalid, the system generates an alarm.

OPEN FILE FORMATS

Where the video is not required for legal purposes, but shared within an organization, consideration may be given to utilize an open file format video export. In this application, exporting to open-format video files (e.g. MP4, AVI) means that users can more easily view exported video using common video players (e.g. Windows Media Player, QuickTime, etc.) As this is an open file format, it is possible to edit and alter the view stream.

VIDEO ADMISSIBILITY FOR LEGAL APPLICATIONS

There are two things that need to be considered with respect to the use of video for legal applications. The watermarking and encryption discussion above addresses the requirements for a digital watermark, which should be applied to all exported video streams. The other aspect for consideration is the use of 360-degree surveillance technology.

The use of 360-degree surveillance technology continues to rise rapidly. Panoramic cameras are a fast-growing video segment because of their ability to capture a dewarped view of an entire area. A 360-degree fisheye and panoramic surveillance camera provides surround view. By creating an all-encompassing, panoramic, or wide-angle 360-degree security view, more data is captured, making these cameras a potential solution for a variety of surveillance applications. At the core of 360-degree surveillance devices is dewarping functionality. Dewarping takes images from a fisheye or 360-degree camera and alters the original shape to enable users to view portions of the full video image without distortion. It makes virtual camera views appear to look like a standard camera image. Dewarping

allows the user to capture a wide area with a single device and have a normal view of an otherwise distorted image. As a result of the software altering the original shape of the view and flattening the views, the authenticity of resulting video has been challenged in court.

Refer to Appendix G for a summary of various VSS technologies for consideration.

3.2.4 Exit Lane Breach Control Systems

Many airports choose to install breach control technologies at their exit lanes to deter, detect, and alert security personnel to unauthorized movement into the Sterile Area. These technologies can be standalone or integrate with existing security systems such as ACS and VSS. The types of systems available vary widely, from open lanes with motion detection sensors to fully integrated, multi-technology portal systems.

For comprehensive guidance on researching, designing, procuring, and installing exit lane technology, see PARAS 0023 – Exit Lane Strategies and Technology Applications (to be published in February 2021).

3.2.5 Reference and Guidance Documents

RTCA under Special Committee 224 has developed [RTCA DO-230J – Standards for Airport Security Access Control Systems](#).¹² This document is a “for-purchase” reference standard.

Also see Safe Skies’ [PARAS 0017 – Access Control Card Technology Guidance](#),¹³ and PARAS 0023 – Exit Lane Strategies and Technology Applications (anticipated in February 2021).

3.2.6 Design Checklist

GENERAL

- Emergency Power/Battery Backup
 - All servers, field control panels, operating stations, portal hardware
 - Credentialing system
- Data and Communications
 - Credentialing system
 - ACS server and workstations
 - Field controller to portal
 - Firewall—ACS to outside systems
- Duress Alarm Locations
 - Passenger screening checkpoints
 - Baggage screening areas
 - Ticketing/rental car counters
 - Concession/retail cash registers
 - Dispatch/communication locations
 - Parking toll booths
- Access Point Locations
 - AOA/SIDA/Secured vehicle gates

¹² For purchase: <https://www.rtca.org/content/sc-224-airport-security-access-control-systems-11>

¹³ For download: https://www.sskies.org/images/uploads/subpage/PARAS_0017_Access_Control_Card_Tech_Guidance.pdf

- Maintenance/personnel gates
- Non-terminal AOA/SIDA doors
- Tenant and maintenance doors
- Tenant facility doors
- Nav aids and FAA facilities
- Cargo facilities
- Perimeter gates
- Material storage areas
- Parking management/tenant safes
- Critical equipment locations
- Biometric Access Control Checklist
 - Potential for additional infrastructure
 - Appropriate biometric and credential technology
 - Environmental protection for readers
 - Phasing Plan – later interoperability

ACCESS CONTROL SYSTEM

- Review the installation location and conditions to select the optimal detection technology
- Develop Basis of Design to define the detection zone(s), access control points, object detection, system redundancy, system monitoring, and system interfaces
- Develop Basis of Design to define the PIDS alarm events
- Identify the locations for power and data
- Provide tamperproof screws for all devices that are accessible to the public
- Provide tamper switches on all panels that are accessible to the public

VIDEO SURVEILLANCE SYSTEM

- Develop functional requirements to define the level of monitoring and area of interest for the surveillance camera
- Develop functional requirements to define the quality and level of recording (resolution and frame rate)
- Identify the mounting locations for the cameras coordinated with the various ceiling elements
- Where expansion of an existing system, verify the software version to ensure the proposed new cameras are compatible with the existing VMS
- Identify the locations for power and data, including networking requirements

3.3 Security Operations Center (SOC)

An SOC is the centralized location for airport security monitoring, command and control, and communications functions. Typically, an SOC will be a 24/7/365 operational space, staffed and designed pursuant to the guidance of the security PDD and the ASP.

The SOC serves as a platform to collect information from a range of sources in order to provide situational awareness for command personnel to control the allocation of security resources. The SOC can coordinate multiple communication links throughout the airport, including police, fire/rescue, airport

operations, off-airport emergency assistance, and secure communication channels to federal, state, and local agencies.

The SOC may be a separate room/facility or can be integrated within the Airport Operations Center (AOC), Emergency Operations Center (EOC), or Integrated Operations Center (IOC).

3.3.1 SOC System Concept

The configuration and functionality of the SOC will depend on its roles and relationship with the various airport response functions, as well as how the SOC staff are trained to perform these functions. Airport police dispatch may occur at the SOC or, if incident response is primarily the duty of municipal or county police departments, dispatch and incident management may be performed in a separate Police Dispatch Center. Either arrangement is workable with the proper information flow, which should be a primary objective of the SOC system design.

3.3.2 Design Objectives

SCALABILITY

Scalability is a measure of the ease with which a facility, system, or elements of a system can be modified in size and capabilities to meet changing performance requirements. For an SOC, this means increasing the size of the facility as needs grow, or expanding technology systems to support additional needs.

RELIABILITY, MAINTAINABILITY, AVAILABILITY

Reliability refers to the ability of the SOC to continue to operate without a failure that compromises the integrity of the overall facility. Reliability is generally expressed as Mean Time Between Failure, which is provided by the manufacturer and derived from the equipment design and manufacturing processes.

Maintainability refers to the capability of the SOC to be subjected to normal preventive and corrective maintenance without compromising the integrity of the overall system. Maintainability is generally expressed as Mean Time to Repair, which is derived from the average time required to repair a failed device.

Availability refers to the capability of the SOC to operate and perform normal functions, such as updates, backups, recoveries, etc., without compromising the integrity of the system. Availability extends Reliability and Maintainability to include equipment operation and 24/7 duty cycle in the airport environment, the effects of operator training, support policies and programs, including servicing and spare parts replacement, and other factors that may not be intrinsic to how equipment is designed and manufactured, but impact how equipment actually performs.

Availability also considers the redundancy of key systems, such as mechanical (cooling and heating), power (using normal/utility and emergency power sources), and networks and communications infrastructure.

INTEROPERABILITY

Interoperability is a measure of how well one or more elements of the SOC are able to work with other systems and components. The interoperability may be in the form of Software Development Kits between applications, or sophisticated interfaces utilizing a software-based information broker. Interoperability is primarily an issue of communications among system components.

LEGACY SYSTEM INTEGRATION

Most airport facilities have several existing systems and supporting infrastructure in place. The two most prevalent types of legacy systems are ACS and VMS. These systems typically have well defined interfaces that allow access to system data. An SOC can employ these assets by integrating with the published interfaces. During the design process, planners should identify what legacy systems should be integrated with the SOC, the extent of the integration desired (e.g., just accept data from the legacy system or have full control of the legacy system), and provide the necessary documentation. This includes interface specifications, equipment locations, etc. Planners should then develop a progressive plan for early integration with critical legacy systems.

3.3.3 SOC Configurations

The SOC is typically located within the airport's Sterile or Secured Area. A secondary/redundant SOC may be located remotely from the terminal in a secure location at the airport. The SOC's general design considerations include sufficient space and support facilities for personnel and IT equipment to facilitate rapid access and dispatch. Secondary or redundant SOC facilities may only require mission-critical capabilities and need not be configured with video walls and other full-service equipment. Additional services generally associated with public safety and first response (e.g., first aid stations, lost-and-found departments, public address systems, paging services, etc.) are often supported via public access facilities.

Situational awareness software that is capable of continually monitoring multiple events; coordinating, categorizing, assessing, tracking, prioritizing, and assigning appropriate response resources; and simultaneously reviewing the developing events for relevant patterns, trends, and correlations, can be consistently modified to support regulatory requirements and forensic analysis. The resulting trend analysis may guide adjustments in policies and procedures. Selecting sensor systems with standard interface protocols will enable evolving predictive algorithms to be deployed to assist operators in preventing incidents. When developing a situational awareness solution, planners should keep in mind that detection is not meaningful without assessment, assessment is not meaningful without response, and response is not meaningful without resolution. Prevention is the desired goal, which may be achieved at any point during the awareness cycle.

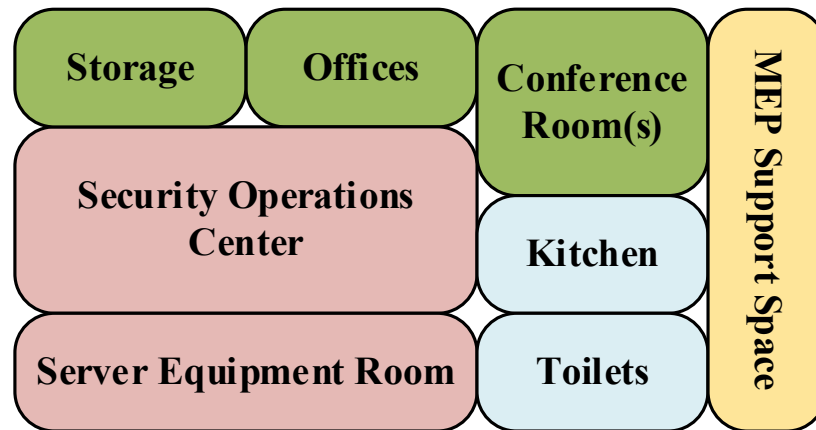
While technology can reach some predefined conclusions and provide options, it is up to an SOC operator to process the multi-sensor data into the optimal response, making necessary adjustments in real time. To assist the operator in making optimal responses, surveillance cameras may also be used for security assessment. Refined data choices, facilitated at the edge by technology as much as possible, are then further analyzed, assessed, and prioritized by the operator for a better-balanced security response, since all security anomalies are not necessarily a risk.

SOCs come in all sizes and configurations—there is no single best design. The space needs to be developed and designed based on the functional requirements identified in the PDD with the constraints of space and budgets.

When considering the operations of the space, Figure 13 illustrates a sample SOC blocking diagram with the various spaces for consideration. The red spaces (Security Operations Center and Server Equipment Room) are the core of the SOC and are recommended for all airports of all size and complexity. The blue spaces (kitchen and toilets) are recommended for the comfort of the operators within the space. The green spaces (storage, offices and conference room[s]) are typically recommended for medium and large airports to provide security managers with direct access to the SOC and security systems, daily

briefings, and emergency operations. The mechanical, electrical, and plumbing support space (MEP) may be adjacent to the SOC or could be remote depending on the needs of the space.

Figure 13. Sample SOC Blocking Diagram



SOC facilities utilize computer-based systems with human-machine interface (HMI) on console- and wall-mounted equipment.

CONSOLE FURNITURE

SOC consoles should permit operators to work in a quiet and efficient manner, utilizing ergonomic interfaces. Appropriate storage space for reference material should be provided at each console position. Consoles should support all voice and data functions of the SOC, along with displays for viewing the ACS, VSS, incident reporting system, and a workstation for email, reporting, and internet access.

Personnel should have the option to stand or sit, and to adjust the lighting on their console. Individual climate control can be provided at each console to enable personalization of ambient workspace conditions. This issue can drive the size and fit-out of consoles and furniture, as well as the scale of the technology procurement, and the balance between operational needs, cost, and support requirements.

INFORMATION/VIDEO DISPLAYS

SOC configurations vary widely depending on the scale of airport operations, operator preferences, functions to be performed, budgets, and other factors.

There are many ways to display information in an SOC, and all available options should be evaluated for the particular requirements of the SOC during the BoD phase of the project. At least two monitors should be provided at each operator station: one for the display of real-time information and a second for event or incident assessment. When several cameras are to be monitored, the addition of a third display will enable an operator to access cameras from a schedule and/or to monitor event and incident logs.

Area displays may use large wall-mounted displays, but the trend is to use video walls. Available monitor technologies include LCD panels, LED arrays, DLP tiles, and rear-projection displays. Each technology has advantages and disadvantages (panel size, resolution, brightness, contrast, flicker, glare, power consumption, reliability, maintenance, and life cycle cost). Video wall configurations typically begin with a grid of monitors (two vertical x three horizontal) and can expand to many times these numbers subject to wall area, power and cooling, aesthetics, and budgetary constraints.

Determining where a large-format video display is located is not as simple as finding empty wall space; one must understand sight lines to manage issues such as light refraction, light levels, and acoustic attributes such as sound transmission and ambient noise management. Placing a display in the wrong

location could result in glare and reflection from windows at different times of day, inhibiting the ability for staff to see details on the screen. In addition to the location, large-format displays require power, cooling, proper wall blocking/mounting brackets, and cabling—elements to address in the design phase. Large-format displays are complex computers that require a similar, high-tech design approach.

Video walls provide a degree of flexibility that cannot be achieved with discrete monitors, provided that such flexibility is included in their design. For example, each panel or segment should be individually addressable from any operator workstation, to permit one event to be stitched across the entire video wall, or multiple events to be displayed on individual panels at the same time. While the screens can be individually controlled, integration with other systems can support displaying video from any source, both inside and outside of the airport.

HUMAN FACTORS AND ERGONOMICS

When designing and operating the SOC, it is important to understand the link between human factors and the ability to absorb information. In high-stress environments like SOCs, every aspect of the environment has an effect on the staff's efficiency and effectiveness. Even minor aspects that cause distraction, inconvenience, or inefficiency to the staff are magnified and can negatively impact operations. A proper human/machine interface for each SOC operator is critical for effective performance, especially under stressful conditions.

- Designs should have staff comfort in mind to reduce stress and improve performance. Lighting should be carefully designed to prevent glare. SOC facilities are not typical office environments, where lighting is often too bright. An SOC facility operator will be visually focused on computer screens and large format video displays.
- Designs should be managed for sound. During emergencies, SOC facilities can become very noisy due to the number of people and the level of activity. Measures such as electronic sound masking and sound deadening materials should be used to avoid aural overload.
- Effective sightlines should be created to provide access to the necessary visual resources, such as video walls and other large-format visual displays. Managers should have unobstructed sightlines to communicate with staff (many times, a gesture or facial expression can be a means of communication in a fast-moving emergency).
- Appropriate seating should be arranged, considering alternate desk and console designs. Ergonomic seating can increase attention spans and reduce repetitive strain injuries. Newer desks, consoles, and seating—such as consoles that move up and down—can reduce fatigue and stress.
- Monitors should be chosen with appropriate resolution, dot pitch, brightness, and contrast to reduce eye strain and increase comprehension. Design of large-format visual displays, such as multi-panel video walls, should be carefully considered, including sightlines from operator stations, lighting, screen resolution, and flicker.
- Traffic patterns should be considered to ensure that staff can move around within the space without causing disruption. Resources such as copier machines should be placed in areas where staff can easily access them without encroaching on others' workspaces.
- Media relationship issues should be considered and the need for public information release to both traditional and social media sources. Many large organizations have created Information Centers to coordinate messages and information flow. In some instances, these centers are segregated near the SOCs and EOCs, with measures taken to prevent unauthorized access to sensitive information.

- If space permits, include an observation area that gives official observers visual and audio access to video walls and other communications. This should isolate sound from the main operational area so that observer discussions are not disruptive. Observer areas may also require escort services for visitors.
- Meeting/breakout room spaces should be included for private meetings, possibly located adjacent to the SOC facility, with glass walls or windows that allow private conversations while maintaining visual contact with the main activities.
- Staff support spaces should be considered, with break rooms in proximity to the SOC facility to accommodate staff. A kitchen will encourage staff to stay onsite rather than leave the facility for lunch or breaks. Sleeping rooms can be useful during long-term emergencies. If the SOC includes an EOC, size these areas for visitors, and plan for overflow personnel to be housed in nearby hotels with shuttles provided.

3.3.4 SOC Infrastructure

To support the high reliability needs of an SOC, the building infrastructure is equally as important as the security systems and operator HMI.

Electrical infrastructure requires adequate capacity and conditioned back-up power. Space should be allocated for a generator outside the facility, and space for a UPS and electrical switchgear inside the facility. If possible, a dual-fuel generator should be used to provide greater alternatives for fuel sources during emergencies. When sizing the generator, the general rules used in normal commercial facilities (where the generator is usually sized only for the minimum capacity to facilitate evacuation of the building) do not apply to SOC facilities. Airports should plan for extended operation using only generator power, and size the generator to support all the key systems that will be required (including HVAC, servers, etc.) The SOC should be able to operate even when local utilities are nonexistent.

HVAC is one of the key needs for the SOC, and is one of the costliest elements to retrofit after construction is completed, so it is better to slightly over-design (to accommodate future expansion) than to under-design and lose that flexibility. Further, planners should consider systems that provide positive air pressure if smoke or other air contamination becomes an issue.

Structural attributes such as blast protection, high wind resistance, or earthquake criteria should be considered when designing new structures. When retrofitting existing structures, blast netting, impact membranes for glass facades, and other accommodations can be used.

Network/internet access should be available from multiple redundant sources. Telephone carriers should be questioned about the availability of dual, spatially separated feeds to the facility. Internet Service Providers should ensure secure connections from multiple sources. Mission-critical traffic should be identified and afforded the highest level of availability, redundancy, and resiliency in network resources. For most SOC applications, this will require IT network availability of 99.99 percent or higher, depending on the network architecture and the network resources required to support the SOC. When this level of network availability is not possible, the SOC design should focus on ways of attaining close to zero downtime for critical security functions, including information flow to incident responders.

Envelope electromagnetic interference and lightning protection should be part of the design, and shielding from electromagnetic pulse may be warranted in certain cases.

To enhance wireless reception inside the SOC, wireless repeaters may be necessary when the building's structure blocks signals. Planners should design for multiband repeaters that will work with all wireless devices being used, both for building Wi-Fi and cellular providers.

3.3.5 Other Design Considerations

AMERICANS WITH DISABILITIES ACT (ADA)

Access to technical spaces is not always required, but, if possible, access for people with disabilities should be provided within equipment room and rack areas. The design should fully comply with the ADA design code requirements regarding all adjacent and support facilities, such as restrooms, aisles, doors, ramps, and emergency elements. Waivers and exceptions may be possible in a technical space, which may mitigate the need for full compliance in all areas.

NEWS AND WEATHER FEEDS

Satellite and cable television feeds should be provided to enable news and weather television channels to be displayed on the wall monitors. Each console position will be able to listen to selected audio on their headsets. If satellite and/or cable feeds are provided, the potential to include broadband access (at least on the cable feed), would be routed differently from the telephone lines into the SOC.

AGENCY INTEROPERABILITY

SOC links to other agencies may involve local, regional, and state assets (EOCs, police and fire, fusion centers, etc.), as well as federal agencies (TSA, CBP, FEMA, etc.), with whom interoperable communications will be necessary. The extent of voice, data, and video streaming interfacing will vary with each organization. Wired and wireless modes of communications will typically be involved, including trunked radio systems used for regional interoperability. Some of these modes may be secured by encryption.

MAPPING

A mapping module has the ability to display multilevel maps and corresponding alarms (e.g., fire alarm, intruder alert, intercom activation, etc.) through the incident management system as they occur. The operator has a visual pop-up icon on the map providing the alarms' exact locations. The operator can alert/dispatch security personnel and emergency first responders as warranted, in addition to monitoring the event through nearby cameras as required. Typically, this would occur through a PSIM (Physical Security Information Management) interface.

COMPUTER-AIDED DISPATCH

When an SOC is primarily an airport police or security operation, a Computer-Aided Dispatch system will often be necessary. The Computer-Aided Dispatch assists operators in responding to an incident and dispatching the correct resources, especially when the volume of activity can easily overwhelm even the best operators. An event anywhere on the airport will cause a notification to the dispatcher: a telephone call via 9-1-1 from any telephone on the airport; a perimeter breach indicator; a fire alarm; or a call from airport operations all would require a prompt transaction response time. Computer-Aided Dispatch could assist during times of maximum load on the system, so there would be no user-discernible degradation of response time.

The Computer-Aided Dispatch system should also provide real-time support for the police, fire, and emergency management services. Operator interfaces should allow dispatchers to access remote data and systems, even from separate systems located on the airport, in another state, or in a federal location, and should support National Crime Information Center (NCIC), E911, voice radio, mapping, video surveillance camera and digital video recording system, ACS, and entry and fire alarm systems.

COMMUNICATION SYSTEMS

An SOC may require multiple communication systems in order to be able to connect with different users within the airport. Typical communication modes and technologies should include:

- Wired telephony as the primary communication with external parties, and should also be considered as backup for IP telephony applications
- Trunked radio talk groups on an 800 MHz radio system
- Commercial cellular telephones for routine activities and receiving alerts
- Standard VHF radios for airfield and air traffic control tower communications

For the wireless communication systems, a wireless radio study should be completed to ensure signal strength and signal penetration. Where signal penetration is weak, consider providing a dedicated radio antenna within the SOC to improve the quality of the signal.

WEARABLES AND INTERNET OF THINGS

Data from wearable sensors will increase as those items become more commonplace. SOC's will need to be able to accept this new data, differentiate and prioritize it along with all other data sources, and process its integration into a usable data stream. Without that selectivity and discrimination, the additional information will present noise to be filtered out rather than contribute to situational awareness.

Internet of Things has implications for how a range of systems (security and non-security) will communicate and work together. This technology development has implications for how situational awareness can be achieved and how command and control operations can be structured. Automated processes may, in certain circumstances, replace human direction.

Drone technology and the use of drones in civil airspace are the responsibility of the FAA. Airports should monitor FAA regulations and establish coordination with the FAA in the event of drone activity.

SOCIAL MEDIA

Social media powers myriad virtual communities in the discussion of a wide scope of topics. Those conversations have implications for a number of organizational functions, including security operations. Understanding and reacting to these conversations can improve intelligence inputs and provide security personnel with situational awareness information to assist in protecting persons, property, and assets.

Recent disasters at airports have demonstrated the importance of social media. Integration of social media into SOC's offers the prospect of significantly changed communications and protocols. Notices and warnings can be sent through social media channels in addition to those currently used. The collection and monitoring of social media content offers the prospect of enhanced situational awareness and threat monitoring. Data can be pulled quickly from the wealth of social media posts. Designers of SOC's of the future would do well to anticipate social media use in their SOC designs.

3.3.6 Trends

Technology trends such as mobile technology (smart phones and tablets), wearables, Internet of Things, social media, robotics and drones offer the prospect of providing command centers with a wide range of additional inputs to strengthen situational awareness. SOC's need to anticipate not only connectivity to these systems to receive their inputs, but also to process the volume of data they offer. Additionally, there is the concern about relaying that data to the existing systems that funnel data into the SOC.

Those trends involve not only substantial new and different information intake; they also present challenges and opportunities for information outflow from the SOC. Integration of social media and exploitation of mobile devices used by employees and passengers presents SOCs with a need for significantly changed protocols. Notices and warnings can be sent through social media channels in addition to those currently used. Information can now be received from a range of mobile devices. SOC designers of the future should anticipate these trends in their SOC designs.

The expanding fields of data collected by growing numbers of cameras and surveillance systems present capacity and cost issues to SOC administrators. Those issues are exacerbated by the addition of new information sources like social media. Cloud computing helps to address those specific issues.

As the volume of data increases, there is a growing challenge to make sense of it. Analytics provide a path forward in making data relevant. Accordingly, SOCs need to look at developments in the field of analytics so that current systems can be configured to accept analytics inputs. This may involve software changes to the entire system, installation of equipment such as cameras that operate analytics at the edge, the integration of audio or motion sensors, or social media monitoring systems that provide alerts or alarms. This analysis of data can assist operators with strategic decision making based on the information processed and presented.

3.3.7 Design Checklist

- Develop operational requirements using the PDD process
 - Identify SOC functions/requirements
 - Identify standards to be adopted
 - Identify legacy systems to retain
 - Identify public access and media needs
 - Identify social media needs in the SOC
 - Identify interoperability requirements
 - Involve IT staff in discussions
- SOC planning and design
 - Establish relation to EOC, AOC
 - Identify limits – space, staff, budget
 - Model SOC at BoD
 - Identify SOC needs for 24/7 services
 - User environment (lights, noise)
 - Backup, power, HVAC
 - Establish cyber security plan
- Determine the SOC user interface with:
 - Operator desk configurations
 - Supervisor stations and functions
 - Redundancy and event management
 - Video wall size and configuration
 - Smart phone accommodations
 - Observer access and isolation

3.4 Baggage Handling System

Baggage Handling Systems (BHS) enable the movement of baggage between passengers and appropriate aircraft. The Checked Baggage Inspection System (CBIS) is an integral part of the BHS to ensure baggage is screened for prohibited items.

When designing a new or reconfigured CBIS, the following issues should be addressed in the design process:

- Preventing prohibited items from entering the Secured Area and being loaded onto a commercial aircraft
- Demonstrating operational flexibility in response to changes in passenger loads, equipment, operational processes, and security levels
- Providing flexibility in CBIS design and configuration to efficiently and effectively utilize the space within the terminal
- Identifying how the CBIS will operate during contingency operations
- Causing minimal interruption or delay to the flow of baggage being screened
- Providing acceptable and comfortable environmental factors, such as air temperature, humidity, air quality, lighting, and noise, particularly in secondary inspection areas
- Coordinating power, data, and video surveillance equipment

3.4.1 Reference and Guidance Document

In order to address these goals, TSA has developed a Planning Guidelines and Design Standards for Checked Baggage Inspection Systems, which provides guidance and design intent for the CBIS. The full version of this document can be obtained at [Planning Guidelines and Design Standards \(PGDS\) Version 6.0 for Checked Baggage Inspection Systems](#).¹⁴

3.4.2 Design Checklist

- Obtain the current version of the TSA *Planning Guidelines and Design Standards for Checked Baggage Inspection Systems*
- Funding design and construction
 - Look for low cost solution
 - Involve all stakeholders
- Three screening levels
 - Level 1 – All bags that fit in EDS
 - Level 2 – Alarmed bags to OSR
 - Level 3 – Unresolved bag search
- Protocols and Concept of Operations

¹⁴ For download: <https://beta.sam.gov/opp/2982dc2e953886ba2f71802b9b46711f/view>

- Checked Baggage Screening Options
 - Fully integrated in-line systems
 - Mini in-line systems
 - Stand-alone EDS/ETD systems
- Vehicle access (e.g., tug, police vehicle)
- Airport-specific alternatives—consider:
 - Airport configuration constraints
 - IT/space/power/HVAC/floor loading
 - CBIS equipment capacity
 - Screening demand data throughput
 - Cost – infrastructure, O&M, staff
- EDS/ETD Key Performance Characteristics
 - Understand system complexity
 - Understand non-reimbursable costs
 - Flexibility to accommodate change
- Consider contingency operations
 - Impact of threat levels
 - Temporary space for bag staging
 - CBRAs
 - Suspect bag retention/removal area

3.5 Security Screening Checkpoint

The Security Screening Checkpoint (SSCP) is a critical element in the protection of the Sterile Area of the airport. Security screening is intended to deter and prevent hijackings and the transport of explosive, incendiary, or dangerous substances or unauthorized weapons aboard commercial aircraft. These threats do not solely come from the ticketed passengers. Airport and airline personnel, concession employees, and concession delivery personnel may also be part of the threat consideration, and may be screened through the SSCP when traveling from public areas to the Sterile Area.

When designing a new checkpoint or reconfiguring an existing checkpoint, the following issues should be addressed in the design process:

- Preventing persons with prohibited items from entering the Sterile Area or boarding commercial aircraft
- Preventing SSCP co-located exit lane breaches
- Securing exit lanes for arriving passengers during both operational and non-operational hours of the SSCP
- Accommodating persons with disabilities who require wheelchair accessibility or allowances for other assistive devices
- Causing minimal interruption or delay to the flow of persons being screened
- Handling tenant goods that cross from the non-Sterile Area to the Sterile Area securely
- Considering leased and non-leased TSA support space needs
- Addressing equipment maintenance and interference spacing requirements

- Demonstrating operational flexibility in response to changes in passenger loads, equipment, operational processes, and security levels
- Having flexibility to accommodate new technology and processes, such as TSA PreCheck and Known Crew Member lanes
- Using terminal space efficiently and effectively
- Providing acceptable and comfortable environmental factors, such as air temperature, humidity, air quality, lighting, and noise
- Having a safe and ergonomic design
- Coordinating power, data, and video surveillance equipment

3.5.1 Reference and Guidance Document

In order to address these goals, TSA has developed a Checkpoint Requirements Planning Guide, which provides guidance and design intent for the SSCP. The full version of this document can be obtained at [TSA Checkpoint Requirements and Planning Guide \(CRPG\)](#).¹⁵

3.5.2 Design Checklist

- Obtain the current version of the TSA *Checkpoint Requirements and Planning Guide*
- Refer to primary TSA guidance documents, including CAD blocks
- Consult with TSA HQ Checkpoint Designer, airport, and airlines
- Planning considerations
 - Level and type of risk
 - Airport operational type
 - Location of SSCP
- Elements of the SSCP
 - Prescreening preparation zone
 - Queuing space
 - Travel document checker
 - Carry-on x-ray
 - Walk-through metal detector
 - Non-metallic barriers
 - Non-metallic ADA gate/access
 - AIT machine
 - Trace detection
 - Private search area
 - Egress seating area
 - Supervisor station
 - Exit lane (if applicable)
 - Checkpoint boundaries
- SSCP signage

¹⁵ For download: <https://beta.sam.gov/opp/6d618178938d8fa31d64fc097587bcb/view>

- Space for TSA staff
- SSCP layout and spacing standards
- Designing for the future

3.6 IT Security

This section outlines high level planning and design considerations for protecting, detecting, and responding to attacks on the airport's IT network, including cyber threats and measures to guard against them in relation to the electronic security systems. Where possible, the airport's IT team should be consulted to the standard IT protection methods that are implemented.

IT systems are widely used as security platforms for airport ACS, VSS, command and control, responder dispatch, and other security functions. With the span of these functional capabilities comes the potential for increased exposure to cyberattacks. Information security exposures are both internal (e.g., insider threats and unintentional breaches of the network) and external, perhaps the most critical being use of the internet and connected IT systems, which rely on the same IT infrastructure used by airport operators.

Planning and design for the physical security of airport IT systems should include multi-layered protection, combined with restrictive user policies and constant security monitoring.

Information for cyber protection is available from several parties. DHS has an extensive cybersecurity program that includes assistance for both governmental and non-governmental entities. NIST has an entire division devoted to cybersecurity; and Airports Council International has set up a Cybersecurity Task Force to develop benchmarks to assist airports with developing programs for dealing with cyber threats.

3.6.1 Information Security and Risk Management

An IT risk-management program involves a cyclical series of best practices and iterative activities that describe the life-cycle approach to cybersecurity, which an airport should consider implementing from the beginning of its IT program.

RECURRENT STEPS OF CYBER RISK CYCLE

- Security Policy – Describe the organization's information protection and privacy objectives, as stated by management and in the PDD
- Privacy – Establish policies, procedures and technological approaches to protect the privacy of personal data and sensitive materials
- Security Architecture – Create a structural blueprint of the technology and processes that will be employed to accomplish the goals of the security policy
- Emerging Threats – Similar to physical threats to airports, cyber threats are continually evolving and should be addressed as part of its risk cycle
- System Prioritization – Develop a ranked inventory that identifies the organization's critical systems and sensitive data.
- Risk Assessment – Conduct a TVA that determines the effectiveness of existing security countermeasures

- Remediation and Implementation – Develop a plan for mitigating each residual risk to an acceptable level
- Security Test & Evaluation – Perform an in-depth validation of the system’s security countermeasures, and create a plan for recurrent testing
- Security Awareness – Implement activities to ensure that all individuals are made aware of their security roles and responsibilities, and back up these policies with recurring training for all departments at all staff levels
- Intrusion Detection and Incident Response – Implement procedures to gather and analyze information to identify potential unauthorized access, and steps to take when it is detected

Like all security, network/data/information security is based on understanding vulnerabilities and threats and identifying which threats can be mitigated. Regardless of the threat type, at least three levels of controls can be considered to mitigate the risks:

- Administrative Control – The security system applications and network shall support the airport’s own security standards, policies, and procedures, including password policy; administrative rights on systems should be limited to those with an administrative role or job function.
- Logical Control – Use software and data to monitor and control access to information and computing systems, e.g., passwords, network and host-based firewalls, network intrusion detection systems, access control lists, and data encryption techniques. Include host-based in addition to network intrusion detection systems, and application whitelisting in addition to access control lists.
- Physical Control – Monitor and control the telecommunications rooms where equipment and infrastructure are located. Use ACS to Secured Areas critical to the airport network.

Information security measures that airports should address:

- Authentication of users and their permissions
- The use of portable devices, and especially flash drives, which can introduce viruses, Trojans, worms, and other attacks on the IT system
- Insider threats that involve airport and airline employees, as well as third parties such as concessionaires, suppliers, and authorized visitors
- Bring Your Own Device policies and connection to the security network

3.6.2 Security Design Issues

The five primary contributing factors to the escalation of cyberattacks in recent years include:

- Utilization of standardized technologies with known vulnerabilities
- IT systems connected to other unsecured networks, exacerbating vulnerabilities
- Insufficient or misconfigured firewall protection
- Lack of or weak encryption of data traversing the network
- Lack of an effective user awareness program, to include policies, procedures, and technologies

IT system designs at airports should include intrusion detection or intrusion protection systems, which is often functionality incorporated into firewall appliances. IT staff may also consider incorporating Data Exfiltration Protection functionality or appliances. The logs from these systems and the firewalls should be reviewed on a regular basis. Airport IT staff should incorporate cybersecurity incident response plans into the other response plans. As with the physical security incident response, these plans should be exercised as tabletops or drills. The incident response plans should also include information about reporting cybersecurity incidents or breaches, and list the appropriate organization.

The security requirements of a particular system and the arrangements made for identifying those risk factors and keeping them within acceptable levels is a critical continuing function, not just a one-time event. New vulnerabilities on existing systems arise almost daily; having a process to address them is paramount.

SYSTEM ARCHITECTURE

Most airport security systems are networked for data distribution to multiple users, with appropriate permission levels and firewalls to safeguard the data, or over a security-only network with minimal secure interfaces to other airport networks. Using cloud-based services for selected functions is an option in both instances. The choice of architecture depends on the scale of security operations (present and future), availability of skilled personnel, facility characteristics such as cable plant paths, and budgetary limitations.

AUTHENTICATION

Information security planning and design should provide means for authenticating users and preventing unauthorized access to an IT network. Unauthorized access to communication and networks can take many forms:

- Authorized individuals failing to log off or re-secure their access points or computers, allowing undetectable access by others
- Authorized individuals gaining access to portions of the network for which they are not authorized
- Unauthorized individuals gaining access to the network from unapproved computers or systems, either by hacking or by using an authorized individual's passwords or access codes, which in turn suggests a need for strong password protocols
- Unauthorized individuals gaining net access through external connections such as modems or wiretaps

Authentication based on what a person has depends on some form of token. Smart cards are the most secure example, but credit cards with magnetic strips and physical (non-cryptographic) keys can also serve as authentication tokens. This form of authentication relies on a device that can read the token, such as a card swipe unit. The main shortcoming of tokens is that they can be lost or stolen and used to authenticate the wrong person. The response to this problem is to combine tokens with passwords or other forms of authentication; for example, ATM cards require PINs in order to function. Authentication that requires a second component is called two-factor authentication. For the most critical systems, three or more factors can be recommended.

CONTROLLING THE USE OF PORTABLE DEVICES

A standard USB port is a widely used means of connecting portable devices to a network, including laptop computers and flash drives. While this is convenient, it also exposes the network to viruses, Trojans, and other types of malware. Planning and design should provide for mitigating such issues by:

- Disabling the USB port completely
- Requiring a flash drive user to log in with a positive means of identification, preferably a biometric identifier
- Requiring system administrator permission before the device can be logged in

Smartphones represent another potentially dangerous means of network access, either via email attachments or by accessing the network using a browser. Vendors have created hardware-based two-factor authentication, combining a password with a token that generates a one-time code. However carrying tokens everywhere means that they can be stolen, and in a large enterprise, tokens are a nuisance to manage.

3.6.3 Legal Issues

The massive amount of data collected by a range of security systems, including ACS and VSS, raises legal considerations that can impact system planning and design. The legal issues generally fall into two categories: what information can be collected and how that information can be used. Security system planners and designers must be mindful of requirements imposed by federal, state, and local laws for the placement of cameras, the types of personal information collected for identity management systems (IDMS), and the safeguarding and dissemination of data. These requirements can vary significantly between jurisdictions, so a legal review of protections for the planned systems by airport counsel is recommended.

EAVESDROPPING

When data or communication infrastructure (wireless or direct connections) is accessible to unauthorized persons, it is susceptible to eavesdropping or interception, as well as corruption of both content and control of data. This threat can be addressed in the planning stages by placement of wiring or conduit in protected routes, placement and orientation of antennae, and encryption of data.

DATA COLLECTION

The principal concern with respect to data collection is privacy protections. The focus should be on the reason data is being collected, and whether it constitutes personally identifiable information (PII) requiring privacy protection. Where that data involves PII or can be readily converted to PII, an organization must be extremely attentive to legal requirements. One mechanism commonly being used is a privacy impact assessment to determine the need for the data collection, which in the case of airport vetting and credentialing, is largely mandated by regulation. Day-to-day collection of data, such as video of public terminals and movement within airport operational areas, may have other considerations.

As a general rule, there is little or no protection under federal or state law regarding the observation of conduct that occurs in a public place, although some state privacy protections are becoming more restrictive. For surveillance systems configured for monitoring only public areas, it is unlikely there will be significant legal implications.

Where surveillance systems are located in areas that adjoin private areas (e.g., private property adjoining airport perimeter), or near public areas where there is some expectation of privacy (e.g., in a terminal concourse near a restroom), there should be efforts made to restrict the ability of SOC operators to observe those areas by means such as restricting PTZ camera coverage or using software to block the views of concern.

Legal issues can also arise where video surveillance is improperly used in a discriminatory fashion or serves to limit the exercise of first amendment rights. These first and fourteenth amendment concerns can be addressed by a system design that allows for supervisory monitoring and audit of system usage.

ISSUES REGARDING DATA STORAGE AND USE

Legal issues concerning data storage and use of data that might affect security system planning and design include the following:

- **Privacy Protection** – Data collected for access control/identity management purposes will clearly be PII with a need for privacy protections in storage of that data, as well as its use and dissemination. Often, state or federal law will impose specific requirements that need to be understood and incorporated into system design.
- **Permissions** – Security system design should provide for the control of internal permissions and authorizations for access to data, and permissions over activities such as copying and disseminating data.
- **Records Retention** – In most jurisdictions, state and local laws treat security and surveillance data as public records to be retained on an established schedule. This means that retention requirements for security and video data may be substantially longer (or shorter) than called for in the airport’s PDD. Video surveillance in particular may add significant costs for lengthy storage.
- **Freedom of Information Act (FOIA)/Sunshine Law Requirements** – As with record retention requirements, FOIA/Sunshine requirements may also be imposed by state and local laws requiring the airport to make accessible certain data that is not governed by PII exemptions. A redaction process can be very time consuming and costly (particularly for video data), with implications for system design as to what data is recorded and stored, how it can be retrieved, and how it is reproduced and disseminated.
- **SSI Regulation** – TSA regulation 49 CFR § 1520 concerning SSI at airports raises significant issues with respect to the safeguarding of video information. Video systems must be configured to ensure that SSI data is properly identified and safeguarded, including permissions and authorizations with respect to access, use, and dissemination of data.
- **Evidentiary Issues** – The evidentiary requirements for the use of security data, particularly video data, will be unique for each jurisdiction. The following should be considered:
 - Airport security normally does not require identification-quality video imagery; in contrast to law enforcement, which needs to identify persons for prosecution. Identification-quality video requires significantly more information than what is necessary for detection, orientation, or recognition, which translates into higher resolution and costlier cameras, lenses, and storage devices.
 - During PDD development, specific locations where identification-quality video imagery will be required should be identified and tagged for schematic design.
 - Video editing should be strictly controlled, with access limited to persons having a valid need-to-know and who have been trained to deal with law enforcement requirements.
 - The video system design should strictly account for the chain of custody necessary to ensure the integrity of video data to be used as evidence.

3.6.4 Reference and Guidance Documents

For additional guidance, refer to [PARAS 0010 – Guidance for Protecting Access to Vital Systems Impacting Airport Security](#).¹⁶

3.6.5 Design Checklist

INFORMATION SECURITY CHECKLIST

- Develop operational requirements using the PDD process
 - Conduct TVA
 - Establish cybersecurity requirements
 - Prioritize IT resources
 - Establish ID interoperability requirements
 - Involve IT department in all discussions
- Complete Information Security Planning and Design Steps
 - Establish multifactor authentication needs
 - Consider multifactor access for critical areas
 - Establish IT security at non-network applications
 - Establish requirements for redundancy and backup
 - Establish cybersecurity requirements
 - Evaluate cloud storage for routine files
 - Address legal and privacy issues

3.7 Coordination

Coordination with other airport systems is critical to the success of deploying an operational security system. This section will identify the major coordination items between disciplines to ensure proper operation in this complex ecosystem. Table 3 provides a typical level of coordination for various security devices. Not all coordination recommendations will be required for each device.

Table 3. Security System Device Coordination

Device	Coordination Recommendations
Access Control System	
Credential Reader	<p><u>Architectural</u></p> <ul style="list-style-type: none"> • Location of the device and appropriate mounting surface • Color of the device <p><u>Electrical</u></p> <ul style="list-style-type: none"> • Equipment backbox location and size <p><u>Civil</u> (where mounted at remote/vehicle entry points)</p> <ul style="list-style-type: none"> • Underground conduit routing
Door Hardware	<p><u>Architectural</u></p> <ul style="list-style-type: none"> • Door hardware based on code requirements • Door locking hardware based on code requirements and security operational need
Control Panel	<p><u>Architectural</u></p>

¹⁶ For download: https://www.sskies.org/images/uploads/subpage/PARAS_0010.SecuritySystemsAccess.FinalReport.pdf

Device	Coordination Recommendations
	<ul style="list-style-type: none"> • Mounting in an accessible location <p><u>Electrical</u></p> <ul style="list-style-type: none"> • Type of power source – normal, emergency, UPS, generator • Power to support the control panel <p><u>Fire Alarm</u></p> <ul style="list-style-type: none"> • Fire alarm relay where required by code <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> • Network data outlet to the appropriate patch panel
Power Supply	<p><u>Architectural</u></p> <ul style="list-style-type: none"> • Mounting in an accessible location <p><u>Electrical</u></p> <ul style="list-style-type: none"> • Type of power source – normal, emergency, UPS, generator • Power to support the power supply <p><u>Fire Alarm</u></p> <ul style="list-style-type: none"> • Fire alarm relay where required by code <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> • Network data outlet to the appropriate patch panel
Server	<p><u>Electrical</u></p> <ul style="list-style-type: none"> • Type of power source – normal, emergency, UPS, generator • Power to support the server <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> • Network data outlet to the appropriate patch panel <p><u>Mechanical</u></p> <ul style="list-style-type: none"> • Environmental conditioning for the installation location
Video Surveillance System	
Camera (interior or exterior mounted to facility)	<p><u>Architectural</u></p> <ul style="list-style-type: none"> • Location of the device and appropriate mounting surface • Color of the device <p><u>Electrical</u></p> <ul style="list-style-type: none"> • Equipment backbox location and size <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> • Network data outlet to the appropriate patch panel
Camera (exterior pole mounted)	<p><u>Architectural</u></p> <ul style="list-style-type: none"> • Location of the device and appropriate mounting surface • Color of the device <p><u>Electrical</u></p> <ul style="list-style-type: none"> • Equipment backbox location and size • Power to support the remote camera <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> • Network data outlet to the appropriate patch panel <p><u>Civil</u></p> <ul style="list-style-type: none"> • Underground conduit and utility routing • Location selected based on avoidance of AOA movement
Control Panel	<p><u>Architectural</u></p> <ul style="list-style-type: none"> • Mounting in an accessible location <p><u>Electrical</u></p> <ul style="list-style-type: none"> • Type of power source – normal, emergency, UPS, generator • Power to support the control panel

Device	Coordination Recommendations
	<p><u>Fire Alarm</u></p> <ul style="list-style-type: none"> • Fire alarm relay where required by code <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> • Network data outlet to the appropriate patch panel
Power Supply	<p><u>Architectural</u></p> <ul style="list-style-type: none"> • Mounting in an accessible location <p><u>Electrical</u></p> <ul style="list-style-type: none"> • Type of power source – normal, emergency, UPS, generator • Power to support the power supply <p><u>Fire Alarm</u></p> <ul style="list-style-type: none"> • Fire alarm relay where required by code <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> • Network data outlet to the appropriate patch panel
Server	<p><u>Electrical</u></p> <ul style="list-style-type: none"> • Type of power source – normal, emergency, UPS, generator • Power to support the server <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> • Network data outlet to the appropriate patch panel <p><u>Mechanical</u></p> <ul style="list-style-type: none"> • Environmental conditioning for the installation location
Video Surveillance System	
Camera (interior or exterior mounted to facility)	<p><u>Architectural</u></p> <ul style="list-style-type: none"> • Location of the device and appropriate mounting surface • Color of the device <p><u>Electrical</u></p> <ul style="list-style-type: none"> • Equipment backbox location and size <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> • Network data outlet to the appropriate patch panel
Camera (exterior pole mounted)	<p><u>Architectural</u></p> <ul style="list-style-type: none"> • Location of the device and appropriate mounting surface • Color of the device <p><u>Electrical</u></p> <ul style="list-style-type: none"> • Equipment backbox location and size • Power to support the remote camera <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> • Network data outlet to the appropriate patch panel <p><u>Civil</u></p> <ul style="list-style-type: none"> • Underground conduit and utility routing • Location selected based on avoidance of AOA movement
Power Supply	<p><u>Architectural</u></p> <ul style="list-style-type: none"> • Mounting in an accessible location <p><u>Electrical</u></p> <ul style="list-style-type: none"> • Type of power source – normal, emergency, UPS, generator

Device	Coordination Recommendations
	<ul style="list-style-type: none"> Power to support the power supply <p><u>Fire Alarm</u></p> <ul style="list-style-type: none"> Fire alarm relay where required by code <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> Network data outlet to the appropriate patch panel
Server	<p><u>Electrical</u></p> <ul style="list-style-type: none"> Type of power source – normal, emergency, UPS, generator Power to support the server <p><u>IT/Comms</u></p> <ul style="list-style-type: none"> Network data outlet to the appropriate patch panel <p><u>Mechanical</u></p> <ul style="list-style-type: none"> Environmental conditioning for the installation location
Physical Security	
Fence / Passive Barrier / Fixed Barrier	<p><u>Architectural</u></p> <ul style="list-style-type: none"> Location of the fence/barrier and visual esthetics Color of the fence/barrier Code requirements for ADA access and spacing <p><u>Civil</u></p> <ul style="list-style-type: none"> Verification of property lines Underground conduit and utility routing Underground soil and ground conditions <p><u>Fire/Life Safety</u></p> <ul style="list-style-type: none"> Egress and access where required by code for emergency vehicles <p><u>Structural</u></p> <ul style="list-style-type: none"> Foundation for fence / passive barrier / fixed barrier
Active Roadblocker	<p><u>Architectural</u></p> <ul style="list-style-type: none"> Location of the active roadblocker and visual esthetics Color of the active barrier Code requirements for ADA access and spacing <p><u>Civil</u></p> <ul style="list-style-type: none"> Verification of property lines Underground conduit and utility routing Underground soil and ground conditions <p><u>Fire/Life Safety</u></p> <ul style="list-style-type: none"> Egress and access where required by code for emergency vehicles <p><u>Structural</u></p> <ul style="list-style-type: none"> Foundation for active roadblocker Foundation for remote power units <p><u>Plumbing</u></p> <ul style="list-style-type: none"> Site and equipment drainage <p><u>Electrical</u></p> <ul style="list-style-type: none"> Type of power source – normal, emergency, UPS, generator Power to support the activation unit of the roadblocker

Device	Coordination Recommendations
Hardened Glazing	<u>Architectural</u> <ul style="list-style-type: none"> Glazing optical clarity <u>Structural</u> <ul style="list-style-type: none"> Attachment method(s) for the hardened glazing
Hardened Structure	<u>Structural</u> <ul style="list-style-type: none"> Attachment method(s) for structural connections Additional structural reinforcement or steel members
Perimeter Intrusion Detection System	
Fence Mounted System	<u>Electrical</u> <ul style="list-style-type: none"> Type of power source – normal, emergency, UPS, generator Power to support the devices <u>IT/Comms</u> <ul style="list-style-type: none"> Network data outlet to the appropriate transmission points <u>Structural</u> <ul style="list-style-type: none"> Foundation for remote equipment cabinets
Radar	<u>Electrical</u> <ul style="list-style-type: none"> Type of power source – normal, emergency, UPS, generator Power to support the devices <u>IT/Comms</u> <ul style="list-style-type: none"> Network data outlet to the appropriate transmission points <u>Structural</u> <ul style="list-style-type: none"> Foundation for remote equipment cabinets
Control Room	
Control Room	<u>Architectural</u> <ul style="list-style-type: none"> Layout of the room Materials and finishes within the room Lighting layout to align with the operator requirements Wall blocking for monitor mounting <u>Electrical</u> <ul style="list-style-type: none"> Type of power source – normal, emergency, UPS, generator Power to support the equipment in the room Equipment backboxes for wall-mounted devices <u>IT/Comms</u> <ul style="list-style-type: none"> Network data outlets to support the various system <u>Mechanical</u> <ul style="list-style-type: none"> Environmental conditioning for the control room <u>Plumbing:</u> <ul style="list-style-type: none"> Fire protection as required by code

3.7.1 Communication/IT Systems

This section focuses on airport communications, specifically networked communications, including cabling infrastructure. These elements are essential to support an airport enterprise architecture that hosts multiple—potentially integrated—security applications such as VSS, ACS, IDMS, and PIDS.

Due to the mission-critical nature of security, it is essential that supporting elements such as communications and cabling infrastructure be designed with high system availability and robust resiliency. Design development should be conducted to eliminate single points of failure at the core and the distribution network layer, and to minimize single points of failure as the system extends out toward the end devices. This is accomplished by providing both equipment and infrastructure redundancy, and high fault-tolerant design techniques where feasible.

The communications network supporting security systems should not only have high system availability, but also should ensure data integrity and data security. Airport operators should ensure that appropriate network information/data security solutions and protocols are incorporated within its enterprise network architecture both at the network level and at the application/session level. Loss of functionality or data integrity in these systems risks jeopardizing the airport's safety and security.

The design process for the IT infrastructure for security systems should examine each element at the earliest possible design stages to ensure a successful supporting infrastructure methodology. The span of departmental communications at an airport will vary with the size and organization of the airport's functions. It is critical at early stages in design to identify the ownership of the IT infrastructure and network communication systems.

3.7.1.1 Reference and Guidance Documents

For additional guidance on airport cybersecurity, refer to [PARAS 0007 – Quick Guide for Airport Cybersecurity](#).¹⁷

3.7.1.2 Coordination/Design Checklist

- Establish ownership of the cabling infrastructure, including patch panel and patch cords.
- Identify category cabling including the EIA/TIA cable wiring scheme.
- Develop bandwidth requirements for security devices based on the edge and core network throughout requirements.
- For common-use networks, confirm the VLAN (virtual LAN) configuration scheme. Typically, a separate VLAN is provided for ACS and VSS.
- Verify if the network will be configured as unicast or multicast. Multicast is recommended for VSS to support multiple simultaneous streams without additional network traffic.
- Locate one (1) data network outlet adjacent to each IP security device. Two (2) data outlets should be considered to enable future expansion.

3.7.2 Electrical/Power Systems

Electrical/power systems are critical to the operation of security system. During the PDD, an assessment should be completed to assess the potential impact of power availability, as well as the integrity of security, communications, operations, and emergency egress systems. At this stage of the design, it should be confirmed how circuiting, redundancy, and backup power sources will support the security systems. This is especially critical as more security systems are migrating from dedicated low voltage (24v) power sources to IP-based communication utilizing Power over Ethernet (PoE) technology.

¹⁷ For download: https://www.sskies.org/images/uploads/subpage/PARAS_0007.CybersecurityQuickGuide.FinalReport.pdf

The electrical/power design should be reviewed with the project electrical engineer. This section is intended to provide general guidance of the power sources.

CIRCUITING

In addressing power circuiting for security systems, it is critical to consider the full communication of the system in order to understand its power needs. An example would be an access control door, which requires power to the electric lockset, the local door controller, the centralized control panel, the network that supports the panels, the access control server, and the SOC workstations. The power circuiting needs for each component should be addressed individually and then as a complete system.

BACKUP POWER SOURCES

Normal circuit power is not protected nor connected to a backup power source. Emergency circuit power is connected to a backup power source (generator) and typically utilized to support life safety systems (fire alarm, emergency communications, etc.) and supported by UPS for the transition from normal to emergency power. It is critical to understand how each backup power source may impact a security system.

UPS are battery-based solutions that are typically used to provide limited backup power during a primary power failure. The uptime power when systems are energized via UPS is limited to the size of the UPS batteries. UPS units are typically used as a power bridge between normal power and an emergency/backup power source. Where the systems are only connected to UPS, the UPS provides an opportunity to safely shut down systems before the battery power is expended.

Generators are the most common form of backup/emergency power for airports. The generator should be sized to either support the connected load at full power or to support critical power loads, including code-required systems and security systems. Most local building codes require generators to come online within 10 seconds after loss of power to support emergency operations. As the generator takes on average 10 seconds to achieve full operation and therefore full power, there is the possibility that the security devices will be offline during this spin-up time of the generator; a UPS is recommended to support security system operation during this spin-up period. Once at full power, the generator can support the power load for as long as a fuel source (diesel, propane, jet fuel, etc.) is present.

It is critical to ensure the generator's supply of operating fuel. A risk assessment should be completed to ensure the ability to deliver fuel during emergency operations.

REDUNDANCY

When planning and reviewing utility services, it is desirable to have multiple feeds (from separate circuits and separate substations where possible) and spatial/geographical separations where multiple feeds exist (particularly regarding singular vulnerability at the actual point of service), to minimize loss of power and airport function.

Consideration should be given to the fact that most airports were built prior to the introduction of contemporary integrated systems; the electric power distribution infrastructure often is not configured to meet current security requirements.

A minimum of two power distributions (buses) should be considered, one for mission-critical systems and one for non-critical functions. The primary goal of electrical system design should be to protect the safety of personnel within the facility and enable safe evacuation or sheltering. The design should also ensure protection of the security system and data network from damage resulting from loss of power.

3.7.2.1 Electrical Grid Dependency

During the PDD development, planning and design should include provisions for backup electrical power appropriately sized for emergencies and outages. It should also provide for alternative power feeds if the area is served by more than one utility, and for routing power around substations in the area.

ELECTRICAL GRID

Most airports depend on external grids for their electrical power, which are operated by municipalities and/or may be privately-owned. Where possible, power from the electrical grid should be fed from two sources to ensure continued operation if one of the sources is interrupted.

CENTRAL UTILITY PLANT

A Central Utility Plant (CUP) typically supplies heating, cooling, and often electricity from a central location. A typical CUP includes boilers, chillers, electrical switchgear, pumps, backup generation, and control systems connected by thousands of feet of underground piping and miles of electrical and data cable, supporting multiple buildings on the airport campus. The typical systems involved are:

- **Boiler Systems** – The function of the boiler is to use fuel to produce thermal energy in the form of steam or hot water and supply it to campus buildings. To achieve this, boilers have controls, burners, fans, and heat exchangers.
- **Chilled Water Systems** – The chiller’s function is to produce a low temperature fluid that can be circulated throughout a campus to provide cooling. Like boilers, the chiller requires energy to make it happen. Components involved in chilled water production include controls, pumps, heat exchangers, and cooling towers.
- **Electrical Systems** – The electrical system represents the primary utility service on which the boiler system and chilled water system rely. Without electricity, other utilities will be inoperable. Major components of a campus electrical system include the utility interconnection, feeder, switches, transformers, and distribution. Some campuses only have the capacity to generate electricity for backing up critical loads. Other campuses have enough electrical generation capacity to provide power to the entire campus, and operate completely independently of the local utility.
- **Distribution System** – The distribution system provides the means by which the thermal energy is transported throughout the campus. The system includes pipes of various sizes and materials, pumps, joints, and valves. Campus electrical generation also requires distribution, which can be above or below ground.

Where an airport does not have a CUP, these systems would be distributed throughout the airport in multiple locations, but would supply and perform the same functions.

MICROGRID

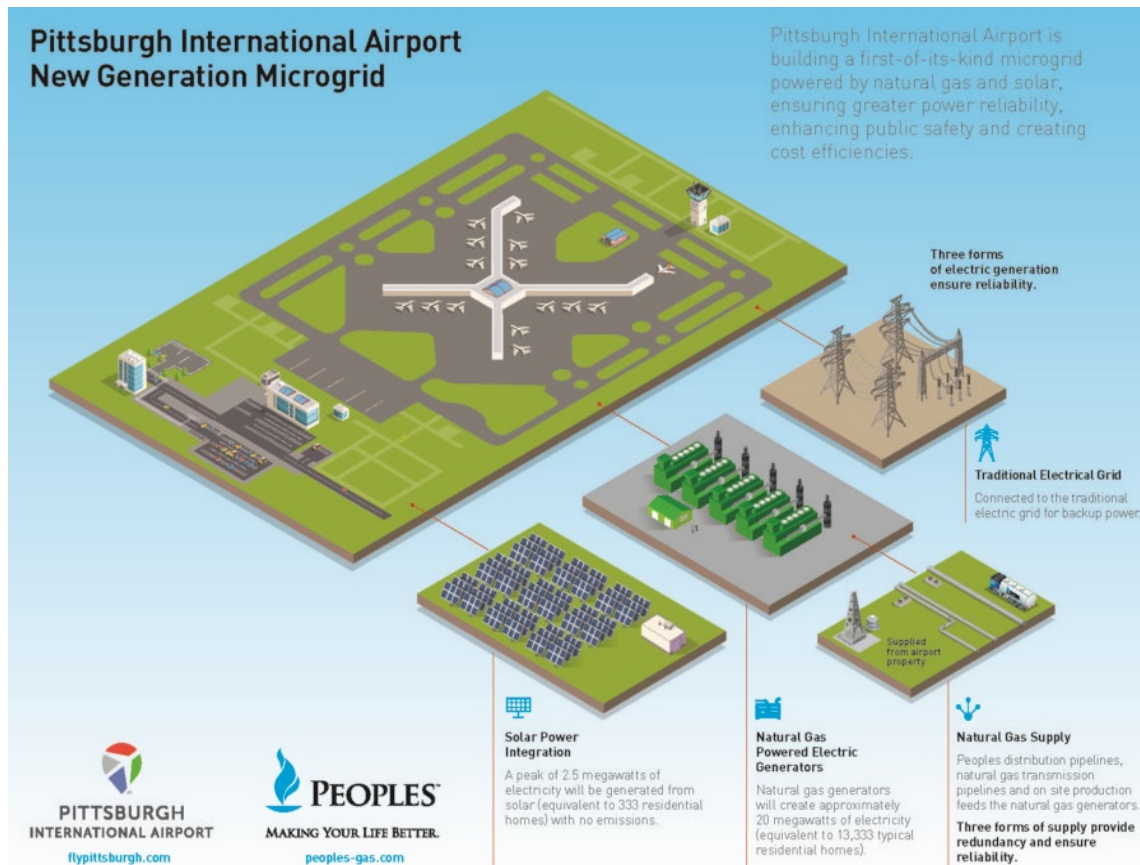
A microgrid is a system of energy sources, energy consumers, and energy storage. This system can operate completely independently from the traditional centralized power grid (macrogrid) in island mode. Alternatively, in the grid-connected mode, it can be a source of power to the macrogrid or it can draw power from the macrogrid as conditions demand.

Microgrids are typically powered by multiple sources. The trend in new/redevelopment terminal projects is to utilize natural resources to generate and store power under this type of electrical configuration. When the sun shines and the wind blows, the microgrid may generate more power than its users need—and even more than it can store—so it transfers power to the macrogrid. On days when solar and wind

energy is not available, it cannot generate sufficient power and may have even run out of stored energy, so the macrogrid is called on to transfer power to the microgrid.

This type of energy system provides power to the airport from multiple sources, which reduces the risk of power loss to the airport, and therefore is a viable risk mitigation measure for threats to utility infrastructure.

Figure 14. Pittsburgh International Airport New Generation Microgrid



Source: Pittsburgh International Airport

3.7.2.2 Coordination/Design Checklist

- Establish power load requirements for security systems
- Identify normal, redundant, and/or backup power sources.
- Identify local power requirements (e.g., door lock) and centralized power requirements (e.g., IT/Security Closet equipment)
- Review power circuiting from source to end device (e.g., backup power from IT/Security Closet network switch, system server, access control panel, and door control panel – ensuring all devices on backup power)

3.7.3 Lighting Systems

At this time, there are no federal government–mandated requirements for security lighting at airports. Industry security lighting standards have been published by the Illumination Engineering Society of North America (IESNA). These standards call for at least 1 foot candle (fc) of luminance for sidewalls

and footpaths, with a uniformity ratio not greater than 4:1 for parking facilities. Lighting should be elevated to 30 feet or more to diffuse dark spots and prevent excessive point illumination. Light color is also a consideration. IESNA uses a color index of 1 to 100, with 100 representing sunlight, and recommends a color index of 50 or more for security lighting.

It is advisable to evaluate lighting in areas monitored by video cameras using a light meter to measure illumination levels, both existing and proposed. The ability of video cameras, and video analytics if implemented, to function properly under these conditions should then be tested in an operational environment.

The placement and amount of lighting, whether interior or exterior, should address basic issues such as point-light sources in the camera's field of view (including streetlights and vehicle headlights at night), reflections from metallic and glass surfaces at various times of day at various sun angles, and the sensitivity of camera-lens combinations. For example, terminals with large glass facades, may at some time during the day be flooded with sunlight to the extent that video cameras in these areas become useless for monitoring areas of the terminal. Being able to control natural illumination consistent with security camera capabilities, using shutters or other means, should be considered.

Supplemental lighting may be needed for video cameras to function properly in areas such as a fenced perimeter that is shielded from the sky by trees or nearby buildings. Where feasible, street lighting can be used to raise the illumination in such areas to a level compatible with camera sensitivity.

Near-infrared illuminators, which produce light that cannot be seen by the naked eye but is visible to most security camera sensors, can be used when visible lighting is undesirable. Near-infrared illuminators located at video cameras are generally limited to short distances because of the attenuation losses in illuminating the target and sensing the reflected light.

The amount of supplemental illumination needed will depend on the area to be lighted, the distance of the illuminator from the observing camera, camera sensitivity, and lens relative aperture. Illuminators should be placed as close to the target area as possible, rather than at the camera, to minimize the power required.

3.7.3.1 Reference and Guidance Documents

For additional guidance on security lighting, see [Illuminating Engineering Society \(IES\) G-1-16: Guideline on Security Lighting for People, Property, and Public Spaces](#).¹⁸

3.7.3.2 Coordination/Design Checklist

- Establish minimum light levels and color index for the surveillance cameras
- Establish minimum light levels for exterior AOA/SIDA entry points to support security operations and identity verification
- Review proposed lighting patterns to minimize shadow areas
- Review interior lighting to ensure light lenses are not directed into a camera field of view

¹⁸ For purchase: <https://webstore.ansi.org/Standards/IESNA/IES16?source=blog>

3.7.4 Mechanical Systems

Mechanical systems are critical to providing an environmentally conditioned space for the protection of active security equipment (e.g., servers, network switches). The mechanical systems should be identified and selected by a qualified mechanical engineer to mitigate the heat output from the active equipment in the IT/Communication Room and SOC.

Typical cooling systems utilized in IT/Communication Rooms/SOC:

- CRAC (computer room air conditioning) units are self-contained devices that typically pump cool air through a raised floor system into the equipment cabinets to lower the temperature of the equipment in the cabinets. These systems are becoming less commonly used.
- A Chilled Water System is a localized air handler system and is more commonly used to provide cooling to IT/Communication Rooms. This system relies on a chilled water supply, typically generated centrally at the airport, which is pumped out to the air handler. As hot air is drawn into the air handler, the chilled water is used to reduce the temperature of the air it expels. What should be considered with selecting this type of system is that the air handler will create condensation, which needs to be drained from the air handler. A blocked drain line could result in water dripping on equipment cabinets. Leak detectors should be considered to detect and alarm on the presence of water.

3.7.4.1 Coordination/Design Checklist

- Establish cooling load requirements for security systems
- Identify if the cooling is on normal, redundant, and/or backup power sources.
- Ensure leak detectors are installed within condensate/drip pans with an alarm contact to the security system and the building management system

3.7.5 Civil Systems

For the purposes of this guidance document, civil systems refer to underground infrastructure services to support the operations of the airport. As part of this system, there are potential security risks to the airport if not properly protected as part of the security system design.

MANHOLE COVERS

Manholes provide access to underground infrastructure that may support cabling or piping systems. Many times, these covers are left unsecured and accessible to the public. It is recommended that manholes located in the public/landside area are secured with a manhole cover lock. Figure 15 is an example of an integrated cover lock and secure key to unlock the cover. Once the lock is released, the hatch can be removed to provide access.

WASTEWATER OUTFALLS

Wastewater outfalls are typically large openings that provide a discharge point of a waste stream into a body of water or larger storm drain collection point. At a minimum, there should be a grate across the discharge point to prevent access into the piping, especially where the piping penetrates an AOA/SIDA perimeter fence.

Figure 15. Manhole Cover Lock



Source: EJ Group

ROADWAY ENCLOSURES

Roadway enclosures are typically communication equipment cabinets located external to the terminal building to extend communication networks to remote devices. These enclosures are usually stainless steel with a key lock and/or latch to prevent access to the equipment and cabling inside. It is recommended that these cabinets be fitted with a door position switch to monitor the status of the cabinet and provide an alarm to the ACS when the enclosure is opened. As an additional level of access protection, it is also recommended that the key lock and/or latch lock is on a proprietary keyway. In addition, where the roadway enclosure can be accessed by a vehicle, bollards are recommended to provide physical protection around the enclosure, as shown in Figure 16.

Figure 16. Roadway Enclosure



3.7.5.1 Coordination/Design Checklist

- Identify locations of underground utility duct banks; for landside locations, consider physical access control protection.
- Identify outfall locations and provide physical protection to prevent entry.
- Identify locations of landside roadway enclosures. Where enclosures contain operational sensitive equipment, consider implementing physical controls and monitoring of the enclosure.

3.7.6 Architectural Systems

For the purposes of this guidance document, architectural systems refers to all fixtures and finishes within the terminal. This section will address the potential requirements for this system and coordination of the security devices within the built environment.

DOOR HARDWARE

Door hardware is typically designed and developed based on the PDD and functional requirements of the door operation, including the security needs. This information is documented in a door hardware schedule and specified in Division 08 architectural specification documents. The Door and Hardware Institute (DHI) has developed a recommended “Sequence and Format for the Hardware Schedule.” The specification documents are typically the responsibility of the architect, coordinated with a DHI-certified architectural hardware consultant.

The DHI document is helpful for anyone in the construction industry working with architectural door hardware. It brings a basic understanding of all the components and how they are applied to work with the total door opening. There are many products, functions, applications, and component combinations available to be specified, furnished, and installed. DHI’s resource helps put order to the scheduling process to ensure all applications, codes, and components are reviewed for proper operation, compliance, and function.

The door hardware schedule should include these items applicable to the physical security of the door and in support of the electronic locking hardware.

- Door number
- Door type (e.g., flush, full-glass, half-glass, or paneled).
- Opening width
- Opening height
- Number of door leaves (e.g., single or pair)
- Door thickness
- Door material
- Frame type (e.g., three- or four-sided, transom, or sidelight)
- Frame material
- Details (e.g., head, jamb, and sill conditions)
- Fire rating
- Hardware group (e.g., lockset type)
- Elevations
- Extra remarks or notes (e.g., security door type reference)

Figure 17 shows a sample door Hardware Set Schedule. The first column of the chart reflects the Set #, which is used to define the hardware associated with the door type. The Set # should include a reference to the type of security devices that will be applied to the door.

Figure 17. Sample Door Hardware Set Schedule

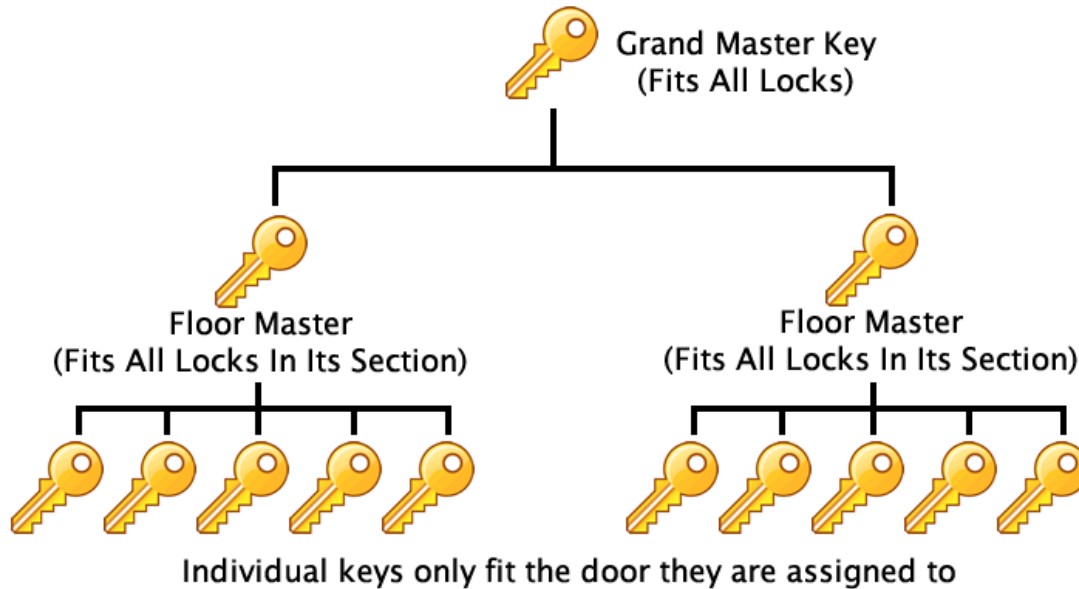
SET #	DOOR TYPE	HARDWARE TYPE	HINGES	#	HANDLE/PULL	#	CLOSER	#	LOCKSET	#	STOP	#	STRIKE	#	FLUSH BOLTS	#	SECURITY	#	
HS-1	TYPE A	ENTRANCE (DOUBLE ENTRY DOORS)	TOP: CENTER PIVOT BOTTOM: CENTER PIVOT	TOP: CRL R/OON 154E OR EQUIV. BOTTOM: CRL R640CB OR EQUIV.	ADA COMPLIANT 3" BLACKENED STAINLESS STEEL RECTANGULAR OFFSET PULL	CAN 3073HEB.32D OR EQUIV.	CRL FLOOR CLOSER	CRL R640C B OR EQUIV.	TBD	TBD	TBD	TBD	TBD	TBD	NA	NA	CARD READER, EXIT RELEASE, DOOR CONTACTS	BY SECURITY VENDOR	
HS-2	TYPE B	ENTRANCE (REVOLVING ENTRY DOORS)	REFER TO CRANE REVOLVING DOOR SPECIFICATIONS FOR MORE INFORMATION																
HS-3	TYPE D	ENTRANCE (DOUBLE LOBBY DOORS)	SINGLE ACTING CENTER PIVOT, TOP & BOTTOM BARRIER FREE, HOLD OPEN	TOP: DORMA P121 W/ 355.9 INSERTS, BOTTOM: DORMA B15-75-9" W/ HOLD OPEN R57.016, OR EQUIV.	ADA-COMPLIANT RECTANGULAR OFFSET PULL	TBD	FLOOR CONCEALED, INTEGRATED W/ PIVOT	SEE PIVOT SPEC	RAIL LOCK	"DORMA" DR3 RAIL LOCK 525-919 OR EQUIV.	CONCEALED STOP	SEE PIVOT SPEC	SPRING-LOADED DUST PROOF STRIKE	"DORMA" R32.033 OR EQUIV.	NA	NA	NA	NA	
HS-4	TYPE E1	PIVOTING WALL PANEL (LOBBY)	CENTER HUNG TOP PIVOT, CENTER HUNG BOTTOM PIVOT	TOP: DORMA B052 HD BOTTOM: DORMA B1588 (W/CLOSER), OR EQUIV.	NA	NA	CONCEALED, INTEGRATED W/ PIVOT	SEE PIVOT SPEC	RAIL LOCK	"DORMA" DR3 RAIL LOCK 525-919 OR EQUIV.	CONCEALED STOP	SEE PIVOT SPEC	SPRING-LOADED DUST PROOF STRIKE	"DORMA" R32.033 OR EQUIV.	NA	NA	NA	NA	
HS-4E	TYPE F	ENTRANCE (VESTIBULE)	SINGLE ACTING CENTER PIVOT, TOP & BOTTOM BARRIER FREE, HOLD OPEN	TOP: DORMA P121 W/ 355.9 INSERTS, BOTTOM: DORMA B15-75-9" W/ HOLD OPEN R57.016, OR EQUIV.	ADA-COMPLIANT RECTANGULAR OFFSET PULL	TBD	CONCEALED, INTEGRATED W/ PIVOT	SEE PIVOT SPEC	CARD READER, FAIL-SAFE DEVICE FOR DOOR RELEASE	BY SECURITY VENDOR	CONCEALED STOP	SEE PIVOT SPEC	FAIL SAFE ELECTRIC STRIKE, HEADER OR FLOOR MOUNTED	TBD	NA	NA	CARD READER, EXIT RELEASE, DOOR CONTACTS	BY SECURITY VENDOR	
HS-4P	TYPE G	PASSAGE (CORRIDOR, VESTIBULE)	SINGLE ACTING CENTER PIVOT, TOP & BOTTOM BARRIER FREE, HOLD OPEN	TOP: DORMA P121 W/ 355.9 INSERTS, BOTTOM: DORMA B15-75-9" W/ HOLD OPEN R57.016, OR EQUIV.	ADA-COMPLIANT RECTANGULAR OFFSET PULL	TBD	CONCEALED, INTEGRATED W/ PIVOT	SEE PIVOT SPEC	NA	NA	CONCEALED STOP	SEE PIVOT SPEC	SPRING-LOADED DUST PROOF STRIKE	"DORMA" R32.033 OR EQUIV.	NA	NA	NA	NA	
HS-4	TYPE H	ENTRANCE (DOUBLE OFFICE DOORS)	BEARING HINGES	MCKINNEY MP879 26D OR EQUIV.	ADA-COMPLIANT LEVER	"SCHLAGE" ND SERIES, RHODES LEVER, OR EQUIV.	SURFACE MOUNTED CLOSER W/ CUSH ARM	LCN 1461 & 1465, 367CONS, OR EQUIV.	PUSH BUTTON AND KEY	"SCHLAGE" ND43PD RHO (ACTIVE LEAF), "SCHLAGE" D118 RHO (PASSIVE), OR EQUIV.	CUSH ARM	SEE CLOSER SPEC	STANDARD ANSI STRIKE	"SCHLAGE" OR EQUIV. (PASSIVE LEAF)	MANUAL FLUSH BOLT ON PASSIVE LEAF	"OLYNN JOHNSON" #18, MANUAL FLUSH BOLT (PASSIVE LEAF)	NA	NA	
HS-7	TYPE I	PRIVACY (HALL, BATHROOM, SINGLE DOORS)	BEARING HINGES	MCKINNEY MP879 26D OR EQUIV.	ADA-COMPLIANT LEVER	"SCHLAGE" ND SERIES, RHODES LEVER, OR EQUIV.	SURFACE MOUNTED CLOSER W/ CUSH ARM	LCN 1461 & 1465, 367CONS, OR EQUIV.	COMBINATION LOCK W/ KEY OVERRIDE	TBD	CUSH ARM	SEE CLOSER SPEC	STANDARD ANSI STRIKE	"SCHLAGE" OR EQUIV.	NA	NA	NA	NA	
HS-8	TYPE I	PRIVACY (TENTANT BATHROOM, SINGLE DOORS)	BEARING HINGES	MCKINNEY MP879 26D OR EQUIV.	ADA-COMPLIANT LEVER	"SCHLAGE" ND SERIES, RHODES LEVER, OR EQUIV.	SURFACE MOUNTED CLOSER W/ CUSH ARM	LCN 1461 & 1465, 367CONS, OR EQUIV.	PRIVACY LOCK	"SCHLAGE" ND46S RHO, OR EQUIV.	CUSH ARM	SEE CLOSER SPEC	STANDARD ANSI STRIKE	"SCHLAGE" OR EQUIV.	NA	NA	NA	NA	
HS-8	TYPE I	PRIVACY (SERVICE RM SINGLE DOORS)	BEARING HINGES	MCKINNEY MP879 26D OR EQUIV.	ADA-COMPLIANT LEVER	"SCHLAGE" ND SERIES, RHODES LEVER, OR EQUIV.	SURFACE MOUNTED CLOSER	LCN 4011 REG AL LHL, OR EQUIV.	STOREROOM LOCK W/ KEY	"SCHLAGE" ND3PD RHO OR EQUIV.	FLOOR MOUNTED	ROCKWOOD #M80	STANDARD ANSI STRIKE	"SCHLAGE" OR EQUIV.	NA	NA	NA	NA	
HS-10	TYPE L	ENTRANCE (LOADING DOCK DOORS)	HARDWARE SHOULD MATCH EXISTING EAST FACADE EGRESS DOOR HARDWARE																
HS-11	TYPE K	ENTRANCE (GARAGE DOORS)	REFER TO RAYNOR GARAGE DOOR SPECIFICATIONS FOR INFORMATION. ALL HARDWARE SHOULD MATCH EXISTING GARAGE DOOR HARDWARE																

NOTE: GC TO COORDINATE HARDWARE WEIGHT REQUIREMENTS WITH THE GLASS AND METAL PANELS.

Figure 18 is the Hardware Schedule, which links the Set #'s to the specific doors within the project. It is critical to ensure that the architectural door hardware aligns with the security requirements for the door location. The specifications for the hardware identified on the Hardware Set Schedule are identified in specification section 087100 – Door Hardware.

doors as these doors are not part of the Facility Maintenance department. The lowest level are the individual keys that provide access to a single door.

Figure 20. Example of Lock/Key Scheme System



In addition to the lock/key scheme, the key should be part of a proprietary keyway to ensure that the key cannot be easily duplicated without the airport approval. Typically, the ability to duplicate keys is limited to approved vendors under strict management and audit of the key inventory and duplication.

REFLECTED CEILING PLAN (RCP)

On new and redevelopment projects, the project architect will usually define and coordinate devices on the ceilings in the RCP. During the design process, camera locations would be coordinated with other ceiling-mounted devices, both in location and distance off the ceiling. This process is critical to ensure camera views are not blocked by ceiling-mounted devices.

In addition to cameras, the RCP would show locations access panels/hatches in hard ceilings. Access panels/hatches (Figure 21) are necessary in hard ceilings to provide access to security door controllers that may be located adjacent to doors. Consideration may be given to monitor the status of these hatches, especially where access from public to restricted areas is possible.

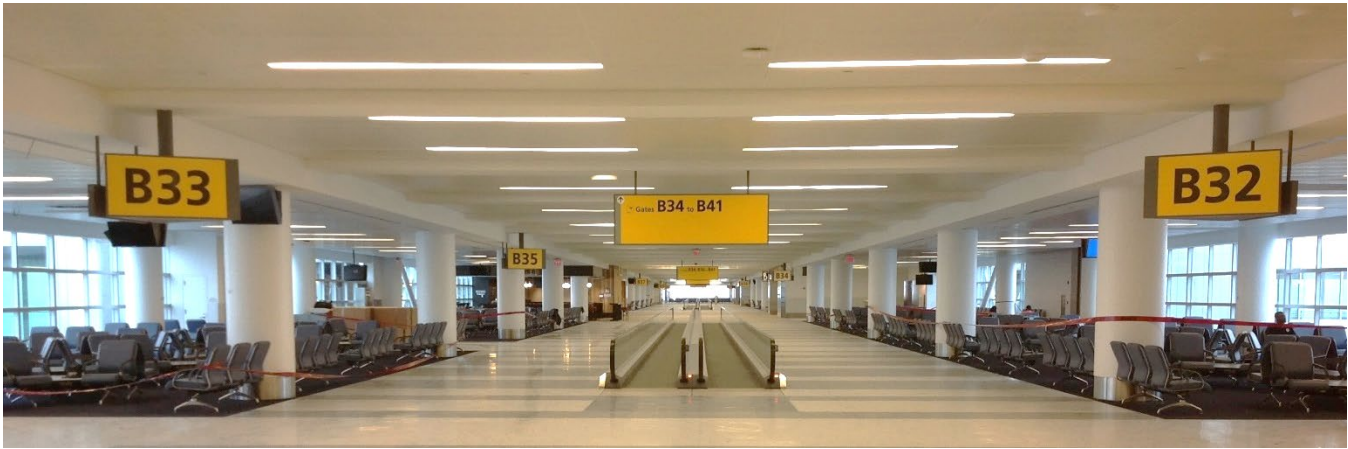
Figure 21. Access Panel/Hatch



SIGNAGE

Airports typically have an extensive and complex array of signage to provide information to passengers. Although signage improves the passenger experience by providing directions, flight information, hold room television news programs, and retail marketing, as shown in Figure 22, it does provide a complex environment for camera locations and achieving the field of view needed based on the PDD requirements. The design and layout of the cameras should be coordinated with the complete signage package to ensure that a camera's field of view will not be blocked by signage. In order to enable any potential relocations of cameras due to late signage installation, a minimum of 20 feet of cabling slack is recommended.

Figure 22. Example of Typical Airport Signage



3.7.7 Coordination/Design Checklist

TERMINAL DESIGN

- Coordinate access point locations and minimize the number of landside to Sterile/Secured Area portals.
- Limit concealment areas/structures and maximize line of sight within the public areas.
- Review different operational pathways based on user groups and access levels, and minimize security boundary crossings.
- Review horizontal and vertical circulation patterns, especially where crossing a security boundary crossing.
- Review public egress pathways, especially when leading to rally points in the Secured Area.

DOOR HARDWARE

- For hard ceiling locations, ensure access hatches are in locations that provide access to door controllers mounted above the ceiling. When possible, consider relocating local door controllers to an accessible ceiling.
- Review door hardware sets, schedule, and specifications to ensure the selected electric locking hardware meets the operational security needs.
- Review the door hardware functions and ensure compliance with national and local egress code requirements.
- Coordinate power and network cabling (for IP enabled locks) to the required locations.

REFLECTED CEILING PLAN (CAMERAS AND SIGNAGE)

- Coordinate security devices with the RCP and all other devices installed on the ceiling. Camera locations should be coordinated with all objects hanging lower than the camera dome (e.g., signage).
- Provide cable slack to enable cameras to be repositioned where needed to account for late additions of ceiling-mounted objects.
- For hard ceiling locations, ensure access hatches are in locations that provide access to door controllers mounted above the ceiling and cameras mounted in the ceiling.

DEVICE LOCATION COORDINATION

- Coordinate security devices with the built environment for consistent mounting heights and locations.
- Review device colors and finishes to ensure alignment with the installation locations and environments.
- Ensure publically accessible devices are secured with tamperproof screws and tamper switches for control panels.

SECTION 4: CONSTRUCTION AND HAND-OVER

4.1 Security during Construction

Construction within airports is a regular occurrence and must consider the regulatory and operational security requirements of the airport. Construction could be as simple as repainting a wall or as complex as the redevelopment of a concourse or headhouse facility. No matter the level of complexity in the construction project, a security representative should be involved with the planning, design/scope of work review, project acceptance, and handover.

PARAS 0037 – Planning and Operational Security Guidance for Construction Projects at Airports is underway, with publication anticipated in late 2021.¹⁹ This section is intended to bridge the gap to that future guidance.

4.1.1 Existing Security Systems

Existing security systems need to remain operational, or an equivalent manual security process needs to be implemented during construction. Capital redevelopment projects provide the greatest risk to existing security systems. The approach taken to protect the integrity of the security systems will depend on the level and type of construction.

SIMPLE CONSTRUCTION EXAMPLE: PAINTING A WALL

In this application, painting a wall could result in the removal of a security device (e.g., card reader or surveillance cameras) in order to complete the painting task. The removal of a camera could result in a blind spot in the remote surveillance of the area. If this is the case, a guard could be posted in the location to provide visual surveillance of the area. Typically, this guard would be a fixed position to act as the security camera, and should not be part of the predefined security patrol unit of the space.

If the work requires the removal of a card reader, this may have a greater impact to security operations. What needs to be considered is the function of the door and the access needs through the door. If there is an alternate route to the space behind the door, it may be acceptable to post a simple sign stating that access through the door on date xx/yy/2020 is not permitted due to maintenance. If this door serves as the primary access point to a secure location, a guard could verify individuals requesting access through the door. This verification may be a manual process of verifying an ID against an approved access list or a more sophisticated process using a remote credential reader for real-time verification.

COMPLEX CONSTRUCTION EXAMPLE: TENANT LEASE SPACE RENOVATION

In a tenant redevelopment of their lease space, security should be aware of the locations of work zone barricades (see Section 4.1.3) and if any existing surveillance cameras will be blocked. Cameras that will be blocked should be relocated to maintain the required level of surveillance of the area, and then returned to the original location after the barricades are removed.

COMPLEX CONSTRUCTION EXAMPLE: CAPITAL CONSTRUCTION REDEVELOPMENT

In this application, a significant part of the airport may be redeveloped or a new facility built. In the redevelopment concept, security should be aware of the locations of both field devices and IT closets where the local access control panels and power supplies are located. This information is documented in as-built drawings, but should be verified, especially where the IT closet supports devices on different floors. This information is critical when construction demolition may impact the operation of the IT

¹⁹ For download (when available): <https://www.sskies.org/paras/reports/>

closet. In this situation, the existing security devices in the IT closet will need to be relocated, re-cabled, terminated, and tested before the IT closet can be removed. Depending on project budgets, consideration may be given to installing new access control panels and power supplies in the new location, which would significantly reduce the anticipated downtime during the cut over from existing panel to new panel location. In either application, security guards should be stationed at regulated access portals to maintain the security of the airport during the period when the devices are offline.

4.1.2 Contractors

Depending on the area, construction may impact security decisions regarding the management of construction contractors and delivery of materials. If the area of work is limited to the landside/public areas, the risk to airport operations is lower and therefore no additional screening protection methods are typically implemented. When the area of work involves access to the Sterile or Secured Area, the contractor will either need to be escorted while in that area or undergo the airport's credentialing process to receive unescorted access to the area.

4.1.3 Work Zones

BARRICADES

Barricades are temporary walls that are used to conceal a construction zone, as shown in Figure 23, preventing disruption to business. Airports are challenged to remain operational 24/7 during construction. Barricades are used to create a protected zone to enable construction to occur and limit public access to the space. The barricades help reduce noise and dust in the passenger zones, and also provide a secure area for contractors to store tools and equipment. When planning the location(s) of the barricade system, several security functions need to be evaluated.

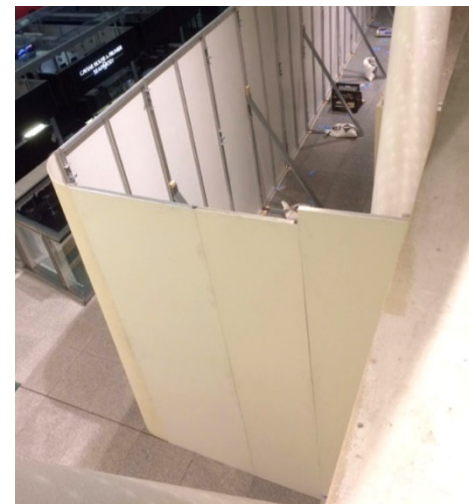
Existing Security Devices:

- Camera locations need to be evaluated to ensure the barricade does not block critical camera views. If this occurs, the cameras should be moved to maintain the required field of view.
- Card reader-controlled doors – where access control doors will be located within the barricade zone, the access requirements of the secure door need to be evaluated to determine if access is required through the door. If the card reader can remain operational, the barricade should allow direct access to the door. If the card reader cannot remain operational and door access is required, a security guard/trusted agent should be positioned at the door to validate and verify individuals requesting access. If the card reader cannot remain operational and door access is not required, a security guard/trusted agent should be positioned at the door to ensure the security integrity of the door.

Security during Construction:

- Typically the contractor will maintain security of the construction zone. This may include a locked construction entrance through the barricade. It is critical that airport security staff has access through the construction entrance door, whether by key or code.

Figure 23. Construction Barricade



Source: Centerstage Barricades

TOOL LOGS

Where the construction activity is occurring in the Sterile or Secured Areas, the contractor should be held responsible to keep a Tool Log, with a copy maintained by airport security. The tool log should specifically identify the tool and its manufacturer, model number, and serial number. The tool log should be checked daily at the start and end of the contractor work shifts to ensure that no tools/prohibited items are introduced into the Sterile/Secured Area. Unaccounted tools need to be reported to airport security immediately for further investigation.

4.2 Testing

Testing is critical to ensure the proper installation, programming, and operations of the security systems per the initially agreed upon PDD, BoD documents, and other project construction documents (drawings and specifications). As with the design process, testing should follow a methodical process to confirm all devices and systems are thoroughly tested before turning the newly installed system over to the client.

TEST AND VERIFICATIONS

Verification by Inspection: This includes examination of an item and the comparison of pertinent characteristics against the qualitative or quantitative standard set forth in the project construction documents. Inspection may require moving or partially disassembling the item to accomplish the verification. Inspection should be made of all equipment installations, locking hardware and lock controls, mounting and wiring of electrical and signal distribution cabinets and components, and mounting and placement of sensors, cameras, etc. to ensure compliance to the specifications and that the overall installation is accomplished in a professional manner.

Preliminary Tests: Following installation, each device should be tested to verify the proper functioning of each component within a subsystem. Each subsystem shall be similarly tested until all detection zones, alarm assessment components, alarm reporting and display, and access control functions have been verified. Any deficiency pertaining to these requirements should be corrected prior to final functional and operational tests of the system. When subsystem verification is complete, the entire system shall be tested to ensure that all elements are compatible and function properly as a complete system.

System Operation Test: Upon completion of the preliminary tests and demonstration of the security system components, conduct a formal test, to be known as the System Operation Test, in which all components and subsystems are demonstrated to operate together as an integrated security system. This test is typically performed over a continuous, multiday period. A test plan and procedures for each portion of the test should be prepared in advance and approved by the testing teams in accordance with the project documents for integrated operation.

Tests upon Completion of Work: At project completion, the system shall be subjected to complete functional and operational tests. When all required corrections have been completed, the system shall be re-tested for the proposed final acceptance testing and inspection date. At a minimum, final tests should include the following:

- Test all central CPUs, peripherals, and all panel control functions
- Test all graphic control and annunciation panel functions and displays
- Test electrical supervision of all input/output sensor and data communication bus circuits
- Test all alarm-initiating devices

- Test VSS components, cameras, servers, network video recorders and monitors
- Test all intercom system components
- Test remote battery and battery chargers
- Test system redundancy
- Test access control system to include tie-in to fire alarm system
- Complete operation tests under emergency power
- Visual inspection of all wiring
- Verification that all required submittals have been provided and have been accepted
- Demonstrate software and programming/reprogramming functions of all microprocessor systems
- Verify system response time

4.2.1 Sample ACS Door Testing Procedure

The following are sample ACS testing procedures. Testing procedures should be developed specifically for the area and systems of work, and should follow the ACS requirements identified and established as part of the PDD.

ACCESS CONTROLLED DOOR (ONE DIRECTION)

- Open door to the full 90-degrees and release. The door should close and secure under the action of the door closer.
- Present invalid/unauthorized ID card to the reader. Ensure that access is not granted and an unauthorized card alarm is received on the ACS.
- Present valid ID card to the reader, enter an invalid PIN. Ensure that access is not granted and an invalid PIN alarm is received on the ACS.
- Present valid ID card to the reader, enter a valid PIN. Ensure access is granted through the secured portal.
- From the secure side of the door, turn handle or depress panic hardware and ensure that the request-to-exit device provides non-alarm egress for doors with single-sided card readers. For doors with card readers on both sides, repeat the steps above.
- Hold the door open for 10 seconds and verify door held open alarm is noted on access control workstation. Hold open time in seconds should be confirmed based on the door location and security requirements.
- Force door open and verify door breach is noted within 2 seconds on the access control workstation. For electric lockset doors, insert a plastic card between the lock and the strike plate so that the door can be closed but not locked; the door can then be pushed open to simulate the forced breach.
 - Confirm that the identified camera alarm call-up function is activated and displayed on the call-up monitor.
 - Re-secure the door and acknowledge the alarm. Ensure the alarm is cleared on the access control workstation.

- For fail-secure doors, activate the fire alarm system and ensure that the electronic lockset provides immediate egress.
- Verify door name/number references on ACS are correct.
- Verify from the ACS that the door can be remotely released from the mapping interface.

4.2.2 Sample VSS Testing Procedure

The following are sample VSS testing procedures. Testing procedures should be developed specifically for the area and systems of work, and should follow the VSS requirements identified and established as part of the PDD.

PTZ CAMERAS

- Verify the pan (360-degree) operation of the camera, both slow/stepped pan and full speed. Verify operation from left to right and right to left.
- Verify zoom in/out on a specific object. Verify the camera auto-focus and auto-iris operation at the full wide angle and full zoom angle.
- Verify the operation of pan, tilt, and zoom simultaneously.
- Verify the camera name and label is correct for the installed location.
- Verify the video is properly stored and can be played back.
- Verify the response time between camera selection and camera display. This should occur in under one-second.
- Verify the response time between the camera and PTZ response control. This response control should occur in under ½ second per PTZ keyboard command.
- For exterior cameras, verify image quality during three periods of the day (morning, afternoon, and night).

4.2.3 Testing Documentation Tools

Testing of security systems should follow a methodical process to ensure all devices and the complete system are fully tested and operationally verified. Documenting the testing process is subject to the tools selected by the client, projects, construction management, etc. Documentation may be as simple as a spreadsheet capturing the testing process and documenting a pass/fail condition, or as complex as a fully online testing documentation tool. An example of this type of platform is Procore,²⁰ which is a cloud-based construction management tool. The advantage to a cloud-based tool is that the testing process and status is centrally located and trackable. In addition, when a defect is identified through the testing process, the party responsible for rectifying the issue can receive an email with the identified issue, site picture, and reason for the issue. Although there is a cost to utilize a cloud-based application, it does provide a smoother and quicker testing and commissioning process.

No matter the testing documentation tool, all tests should be signed (physically/electronically) by the testing agent and owner/owner's representative, and include all participants for record.

²⁰ <https://www.procore.com/>

4.3 Training

Training is a critical part of the final acceptance of a security project, whether a small upgrade or full system install or replacement. The training should account for and provide technical services and materials to instruct operators, maintenance personnel, and programmers/database setup personnel to operate, maintain, and program the system. Training should be hands-on and, when possible, on the actual system configured to the client's configurations.

At the completion of the training programs, the security contractor should provide a certification drafted on the contractor's company letterhead stating that client's staff has been trained in accordance with the contract documents and manufacturer's standards and are fully proficient in the operation of the newly installed system.

4.3.1 Levels of Training

The type of training should be configured based on the role of the trainee. Example of these levels may include:

System Operator: This would provide training on how to view device status via the monitoring software, view and clear alarms, check on the status of an ID badge holder, and change the status of a door (e.g., active, bypass, off-line).

ID Office Operator: This would provide training on how to create a new badge holder record, modify a badge holder record, activate/deactivate a badge, and assign permissions to access control portals.

System Manager: This would provide the basic operator training, with additional training to create new devices within the software application, delete devices within the software applications, create, manage and run reports, create/delete operator accounts, and upgrade software applications when approved for deployment.

Database/Software Manager: As most security systems operate on a database platform, typically Microsoft SQL, this training is highly specialized in the development, management, and repair of database applications.

4.3.2 Train the Trainer

As with any role at the airport, staff turnover is possible. It is therefore recommended to create a "train the trainer" program for the systems to ensure consistent and appropriate dissemination of information on the use and operations of the systems to new staff. This may be achieved by a dedicated and competent leader within the department, or training sessions could be recorded with voiceovers and recorded screen sharing. Either method should be included as part of the scope of work for the contractor who is responsible for setting up the initial systems.

4.4 ORAT

There is always a high degree of risk associated with the opening of any new public facility. Operational Readiness Activation & Transition (ORAT) provides a framework for managing the risk of opening a new, or substantially upgraded, large/complex operation. The central purpose of operational readiness is achieving complete readiness, not just construction ORAT. Typical project focus is on construction delivery and completion of a static asset; operational readiness is focused on the business operation, integrating all of the diverse moving parts into one cohesive, dynamic operation.

ORAT typically involves testing of new systems under realistic operational conditions, with participants testing multiple systems simultaneously. An example of an ORAT test could involve the opening of a new concourse. Participants are provided specific roles—e.g. business traveler, family group, airline gate agent, maintenance, etc.—with a goal of having different participants trial different systems, processes, and procedures. For security, this may include breaching a SIDA door to test the operator, camera call-up features, security dispatch timing, and return to normal procedure.

From a security perspective, it is critical that the ORAT manager involves the airport's security department to ensure that policies and procedures identified in the ASP, along with the initial design considerations within the PDD, are fully tested to verify and approve the ability to secure and operate the space.

4.5 Owner Acceptance

With the completion of installation, device testing, system testing, and ORAT testing, the final phase is owner acceptance. During this phase of the project, the systems are turned over to the owner for operation. It is also typically the start of the maintenance and warranty period, but owners should be aware that, depending on how the initial contract was developed, the maintenance and warranty period may be at beneficial use. Beneficial use is when the owner first uses the system or a subsystem for operational purposes (excluding training or testing). This needs to be clearly defined in the request for proposal documents for the system(s).

4.5.1 License Transfer

Security systems, as with any software-based application, require a license provided by the manufacturer. Initially, these licenses are purchased in the name of the authorized security contractor. At the completion of the project, the license should be transferred into the name of the owner. This will provide the owner with the ability to track the status of the license for software updates, as well as select an alternate approved contractor to support and maintain the system.

4.5.2 Record/As Built Drawings

At the completion of the project, the contractor shall provide a copy of record/as built drawings. These documents should reflect the actual and final installation conditions for the systems, and show every change from the original specifications and contract drawings through final acceptance.

All security devices, including those that are located above ceilings or behind accessible panels, should be reflected on these documents. Tagging and labeling on the drawings should be consistent with the labeling utilized within the security systems.

The drawing should be presented to the owner in both hardcopy and electronic version. The electronic version should include the native file format that the drawings were created (e.g., AutoCAD, Revit, MicroStation), along with PDF format. The native file format should identify the version of software used to create the files and all referenced files should be included.

4.5.3 Operation and Maintenance Manuals

The contractor shall provide copies of the approved operation and maintenance manuals for the systems installed, which would include copies of approved shop drawings, equipment literature/cut sheets, bulletins, performance charts, equipment and engineering datasheets, and typewritten instructions

relative to the care and maintenance of the equipment. At a minimum, each manual shall have the following contents:

- Table of Contents
- Maintenance
- Maintenance instructions
- Replacement charts
- Preventive maintenance recommendations
- Troubleshooting charts for equipment components
- Testing instructions for each typical component
- Two typed sets of charts indicating equipment tag number, location of equipment, and specific equipment service
- Instructions for ordering spare parts, including name, telephone number, and address of where they may be obtained.
- Manufacturer's Literature
- The equipment for which shop drawings have been submitted and approved
- Wiring diagrams
- Installation drawings
- Manufacturer's representative and contract information
- Guarantees

4.6 Operation

Upon completion of all testing, training, and final documentation handover, the system enters the operation phase where the owner will utilize the system as part of their security operations. As with any device, regular maintenance is required to ensure the systems are operating at peak performance. Failure to properly maintain the systems will lead to premature failure of components, exposing the security system, and therefore the airport, to risk factors.

4.6.1 Maintenance

Typically, the contractor who initially installs the security equipment is responsible for providing ongoing repair, scheduled maintenance, warranty repair, and maintenance support to the owner for the installed systems for the first year after owner acceptance. The owner may define the response time along with the required hours of service support. Airports will usually require 24/7 support with an average response time of 4 hours. This support window may be increased or decreased, which will impact the cost for the support. Maintenance activities include:

- Routine preventive maintenance consisting of site visits for inspection and adjustment at least once every calendar month for the year after final acceptance of the installation
- Execution of software upgrades during the warranty period when approved to be installed

A factory field service force should be capable of performing all needed inspections, training personnel to service equipment, and providing other services as might arise in relation to equipment servicing.

4.6.2 Life Cycle

As with any electronic component, devices will reach end of life, at which point the device is beyond repair and needs to be replaced. As budgets for equipment are typically identified 12 months in advance, an appropriate life cycle replacement plan should be developed. As a priority, any components with moving parts (e.g., PTZ camera, workstation, server, etc.), equipment batteries (e.g., UPS, batteries on control panels, etc.) and high usage electronic devices (e.g., network switches) should be on a regular replacement cycle. Recommendations for each of these classifications of components are as follows:

- Components with moving parts: 4 years
- Equipment batteries: 1 year
- High usage electronic devices: 5 years

Although the equipment may still be operational beyond the above dates, the costs associated with maintaining these systems at optimum performance may well exceed the cost to replace the component. In addition, failure to perform regular maintenance on the systems will also greatly reduce their operational life expectancy.

4.7 Coordination/Design Checklist

SECURITY DURING CONSTRUCTION

- Clear and defined area of work is identified along with the security expectations for work within the area
- Tool logs are developed to account for all tools, especially those that would be considered prohibited items
- Escort procedures, where required, are identified, and established
- Impacts to existing operational security systems and mitigation/alternate security measures are identified

TESTING

- All devices are tested per the operational requirements as defined in the PDD
- All integration between devices is tested per the operational requirements as defined in the PDD
- All devices are stress-tested, e.g., creating multiple simultaneous alarm events to ensure the alarm traffic load can be received at the operator workstations
- Where the security systems are connected to an emergency power source (e.g., UPS or generator), the systems should be tested under both normal and emergency power
- Where security servers operate in redundant modes, the failover and recovery between the servers should be tested

TRAINING

- Appropriate is training provided for staff based on the position/role within the organization
- Train the trainer videos are created to address future training needs and recurrent training needs

ORAT

- Security scenarios are submitted to the ORAT team for incorporation into the operational trials
- Security scenarios align with the system requirements identified in the PDD

OWNER ACCEPTANCE

- System licenses are transferred to the owner
- All record/as-built documents are provided to the owner

OPERATION

- A regular system maintenance schedule is established with an approved contractor
- Security devices are tested to ensure operating per specifications of the manufacturer
- Life cycle replacement plan and associated costs are established

APPENDIX A: DEFINITIONS

The following definitions provide additional clarity for terms that are not already defined within the respective section where initially referenced in this guidance document.

General Airport Areas

Landside

Landside represents all public areas on the airport prior to the SSCP or a perimeter control point leading to the Secured Area/AOA. It includes the terminal areas prior to the SSCP, patron and other public parking areas, walkways, public access roadways, rental car facilities, taxi and ground transportation staging areas, and any on-airport hotel facilities. Since the landside includes all non-airside areas other than the terminal(s), its location is determined by the airside and perimeter boundary.

Terminal

An airport terminal building is designed to accommodate the enplaning and deplaning activities of aircraft passengers. Larger airports and those with GA areas often have more than one terminal. For the purposes of this document, the term terminal typically refers to the main building, or group of buildings, where the screening, boarding, and unloading of public, scheduled commercial aircraft passengers and property occurs.

Airside

Airside represents the areas of the airport with aircraft movement and ground services that support the aircraft (e.g., baggage, fuel, catering). Airside typically starts at the Sterile side of the SSCP and extends to the perimeter fence/boundary of the airport.

AOA

An AOA is a portion of an airport, specified in the ASP, in which the security measures stipulated in 49 CFR § 1542 are carried out. This area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas used by aircraft regulated under 49 CFR §§ 1544 and 1546, and any adjacent areas (such as GA and cargo areas) that are not separated by adequate security systems, measures, or procedures. This area does not include the Secured Area.

Secured Area

A Secured Area is a portion of an airport, specified in the ASP, in which certain security measures specified in 49 CFR § 1542 are carried out. This area is where aircraft operators and foreign air carriers that have a security program under 49 CFR § 1544 or 1546 enplane and deplane passengers, and sort and load baggage. It includes any adjacent areas that are not separated by adequate security measures.

SIDA

A SIDA is a portion of an airport, specified in the ASP, in which security measures outlined in 49 CFR § 1542 are carried out. Specifically, it is an area requiring display of an authorized ID media.

Regulations do not require a SIDA to have access controls, so it cannot, by itself, be a Secured Area. However, a Secured Area requires ID display, so it is always a SIDA. SIDAs may also lie within AOAs. Generally, the airport operator has the responsibility to secure SIDAs and prevent or respond immediately to access by unauthorized persons and vehicles.

Sterile Area

At an airport with a security program under 49 CFR § 1542, the Sterile Area of the terminal typically refers to the area between the SSCP and the loading bridge and/or hold room door leading to the aircraft.

The Sterile Area is controlled by inspecting persons and property in accordance with TSA screening protocols and a TSA-approved ASP. The primary objective of a Sterile Area is to provide a passenger containment area, preventing persons in it from gaining access to weapons or contraband after having passed through the SSCP and prior to boarding an aircraft.

Aircraft Movement Areas

Aircraft movement areas (runways and taxiways) are completely airside, are required to be within the AOA or Secured Area, and require specific security measures per TSA regulations, as well as adherence to appropriate Federal Aviation Regulations.

Exclusive Use Area

An exclusive use area is any portion of a Secured Area, AOA, or SIDA, including individual access points, for which an aircraft operator or foreign air carrier that has a security program under 49 CFR § 1544 or 1546 has assumed responsibility for security as required under 49 CFR § 1542.111.

Within the exclusive use area, the responsible signatory aircraft operator or foreign air carrier must perform security control requirements described in the exclusive area agreement. The aircraft operator, not the airport, may control access and movement within the exclusive area.

Airport Tenant Security Program (ATSP) Area

An ATSP area is an area specified in an agreement between the airport operator and an airport tenant that stipulates the measures by which the tenant will perform stated security functions, authorized by the TSA, under 49 CFR § 1542.113. ATSPs are similar to exclusive use areas, except that tenants are not regulated parties.

User Groups

Users and Stakeholders

The airport operator and air carriers have the primary responsibility for protecting their passengers and employees. In many cases, they share those procedural responsibilities with other organizations, such as at the screening checkpoint, which is a TSA responsibility, and where TSA has some very specific design requirements. Other federal stakeholders such as Customs and Border Protection (CBP) also have unique operating regulations and security requirements to be introduced early in the host airport's planning and design process.

Other users and stakeholders include virtually everyone with access to the airport, although each area may operate differently for various reasons. It is important to note that, while the prevailing concept in providing airport security has always been protection of passengers and aircraft from terrorist activities, it is an equally important function of the security designer to consider protection from all common criminal activity, including theft, assault, robbery, vandalism, and a multitude of other day-to-day concerns.

The following are examples of airport security users, most of whom have associated access control requirements. All require serious consideration during the planning and design of airport facilities. Some represent greater or fewer security requirements than others; all will affect how the facility in which they function operates. Their concerns are discussed throughout the document:

- The passenger is the primary user of the terminal building and, along with the aircraft, is the underlying reason for security measures to be in place.

- Coupled with passengers are the general public and “meeters and greeters,” who tend to populate the public side of the terminal building or the terminal curbside areas. They are important security concerns both as persons to be protected and possibly as threats.
- Airport and airline employees must have access to various security-related areas of the terminal building to perform their responsibilities. However, not all employees require full access to the entire terminal building and all related facilities.
- Federal agencies primarily have regulatory roles, including but not limited to passenger and baggage screening, customs and immigration functions, and regulatory compliance oversight and inspections. Each will require various levels of access to different secured facilities, and occasionally to all areas.
- Law enforcement, usually a function of a local political jurisdiction, typically has airport-wide responsibilities requiring full access to all facilities and areas at all times.
- Concessions can be in the public, Sterile, or Secured Areas, and may require design accommodations that enable certain users to have access to limited service areas to screen materials and/or move across security boundaries.
- Cargo operations are usually remote from the main terminal building areas, and will often have separate security design requirements unique to each operator. However, each cargo operation must remain consistent with the ASP and evolving regulatory requirements, particularly screening requirements for cargo to be carried on passenger aircraft.
- Tenants may or may not be aviation-related organizations, and depending on their operations and location in relation to Secured Areas, may have additional specialized security requirements beyond what is required in the ASP. Some airports have light industrial zones where the main operations occur within Secured Areas. However, tenants in such areas may have a continuing need to bring items through the airport’s security perimeter for shipment. Similarly, avionics repair shops located in a remote hangar may require access to aircraft to install and test their work.
- Fixed Base Operators (FBO) for GA aircraft are most often found well removed from the main terminal complex in large airports. However, in smaller airports the FBO often operates from an office or area inside the main terminal with direct access to the Secured Area and/or AOA. Furthermore, the FBO has responsibility for managing the security concerns surrounding both locally based and transient GA persons and aircraft, still within the requirements of the ASP.
- Service and delivery include persons with continuous security access requirements, such as fuel trucks, aircraft service vehicles, and persons with only occasional needs, such as concession delivery vehicles or trash pickup. If these service areas become issues for terminal access, some services may be removed to the airport perimeter.
- Emergency response vehicles and personnel might come from dozens of surrounding communities and facilities to provide mutual-aid services in the event of an emergency. This fact drives design considerations for ease of perimeter access, direct routes, and access to affected facilities. Quick access to terminal emergency equipment such as water standpipes, electrical connections, stairwells, HVAC facilities, and elevator machine rooms should also be considered. All of these should be considered in the emergency plan.

Threat Vulnerability Assessment

Risk (General)

The potential for loss, damage, or destruction of an airport asset occurs when systems, processes, and procedures have a vulnerability that a given threat can exploit or attack.

Risk (ISO 31000:2018)

Uncertainty on achieving a business objective. Risk is also a deviation from an objective, which can be either positive or negative. Objectives can be from the financial, quality, project, process, program, transactional, or supply chain.

Risk Analysis (ISO 31000:2018)

Process to understand the nature of risk and determine the level of risk. Risk analysis is the basis for the risk evaluation and decisions about risk treatment and risk management. It is also the systematic examination of risk components and characteristics.

Threats (General)

Specific activities that can damage the airport and its facilities, and cause employee and/or passenger injury or death. Threats include any actions that detract from the overall safety and security of the airport and its operation. A threat can include a bad actor (an insider or outsider) who may wish to cause harm, ranging from extreme examples of terrorist-initiated bombs or hostage-taking to common events such as theft of services, gun and drug trafficking, pickpocketing, graffiti, and vandalism.

Threats (ISO 31000:2018)

Natural or man-made activity with the potential to cause damage, injury, or loss.

Vulnerability (General)

Weakness or gap in an airport security system, program, and/or process that can be exploited by threats to gain unauthorized access to an airport asset or leave the airport susceptible to some form of security hazard.

Vulnerability (ISO 31000:2018)

Susceptibility of the enterprise to a risk event related to the entity's preparedness, agility, and adaptability.

Security Risk Analysis

The process of making an assessment of security risks that considers how likely is it that an event will result in a particular consequence (usually the most credible or worst-case consequence).

Security Risk Assessment (SRA)

A formal process of security risk analysis to document security-related risks over a defined scope of locations and/or activities, and in the light of organizational criteria.

Security Risk Assessment—Asset- or Project-Based

An SRA with a specific and restricted scope to focus on specific assets and/or projects at a high level of detail. This level of granularity can assist security managers and senior managers to manage specific risks and threats.

Security Risk Assessment—Enterprise

An enterprise SRA (ESRA) covers an entire enterprise (as opposed to particular business units or assets within an organization) with the key objective being to protect organizational capabilities.

APPENDIX B: ONLINE RESOURCES AND REFERENCES

Document Name	Issue Date	Version	Issued By	Website	Availability
Airports Council International - Landside Security Handbook	2018	First Edition	ACI	https://store.aci.aero/product/landside-security-handbook-first-edition-2018/	For Purchase
American National Standards Institute (ANSI) ANSI/IESNA RP-104			ANSI	https://www.ansi.org/	For Purchase
American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE)			ASHRAE	https://www.ashrae.org/	Public
American Water Works Association, AWWA J100-10 (R13) Risk and Resilience Management of Water and Wastewater Systems (RAMCAP).	2013		AWWA	http://www.orwarn.org/files/Morley-RAMCAP%20Basics.pdf	For Purchase
ASCE 59-11 Blast Protection of Buildings	2011		ASCE/ SEI	https://sp360.asce.org/PersonifyEbusiness/Merchandise/Product-Details/productId/232616700	For Purchase
Assessing Homeland Security Risks: A Comparative Risk Assessment of 10 Hazards	December 2015		Homeland Security Affairs	https://www.hsaj.org/articles/7707	Public
ASTM F2656—07 Standard Test Method for Vehicle Crash Testing of Perimeter Barriers, American Society for Testing and Materials (ASTM)		F2656/ F2656M	ASTM	https://www.astm.org/Standards/F2656.htm	For Purchase
ANSI/BICSI 007-2020, Information Communication Technology Design and Implementation Practices for Intelligent Building and Premises	July 2020		BICSI	https://www.bicsi.org/standards/available-standards-store/single-purchase/bicsi-007-iot-intelligent-building	For Purchase
Building Security: Handbook for Architectural Planning and Design	April 2004		McGraw-Hill Professional	Available for purchase from internet book sites	For Purchase
Global Social Media Research Summary	August 2020			https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/	Public

Document Name	Issue Date	Version	Issued By	Website	Availability
Checkpoint Requirements and Planning Guide	December 2018	0	TSA	https://beta.sam.gov/opp/6d618178938d8fa31d64fc097587bcbb/view	Public
Chemical & Biological Agent Resources and Guidance				May be obtained from TSA, FEMA, FBI, Department of Energy (DOE), Center for Disease Control and Prevention (CDC)	Public
Guidelines for Secure Use of Social Media by Federal Departments and Agencies	September 2009	1.0	CIO/ISIMC/ NISSC/W2 OSWG	https://www.energy.gov/sites/prod/files/maprod/documents/SecureSocialMedia.pdf	Public
CISA Insider Threat Programs for the Critical Manufacturing Sector – Implementation Guide	August 2019	0.0	DHS	https://www.dhs.gov/sites/default/files/publications/19_0830_cisa_insider-threat-programs-for-the-cm-sector-implementation-guide.pdf	Public
Common Use Passenger Processing Systems (CUPPS)	July 2018		IATA/A4A/ ACI	https://www.iata.org/contentassets/1dccc9ed041b4f3bbdcf8ee8682e75c4/cupps-rfp-guidance-document-july_2018.pdf	Public
Personal Identity Verification (PIV) of Federal Workers and Contractors			CSRC	https://csrc.nist.gov/projects/piv https://csrc.nist.gov/publications/detail/sp/800-79/2/final https://csrc.nist.gov/csrc/media/publications/fips/201/1/archive/2006-06-26/documents/fips-201-1-chng1.pdf	Public
Cybersecurity Curriculum Resources			NICCS	https://niccs.us-cert.gov/formal-education	Public
Deliberative Risk Ranking to Inform Homeland Security Strategic Planning	April 2016	Volume 13 Issue 1	Homeland Security Affairs	https://www.degruyter.com/view/j/jhsem.2016.13.issue-1/jhsem-2015-0065/jhsem-2015-0065.xml?format=INT	Public
Design Considerations for Airport EOCs - Research Report - 189	2018		ACRP	https://www.nap.edu/catalog/25280/design-considerations-for-airport-eocs	Public
DOE Vulnerability and Risk-Assessment Methodology	2001		DOE	https://www.eisac.com/	Public
e-CFR Aircraft Operator Security	September 2019	Part 1544	e-CFR	https://www.ecfr.gov/cgi-bin/text-idx?SID=5a1b08bbf0c88da7072c6659eb56b91f&mc=true&node=pt49.9.1544&rgn=div5	Public

Document Name	Issue Date	Version	Issued By	Website	Availability
e-CFR Airport emergency plan	September 2019	Subpart D → §139.325	e-CFR	https://www.ecfr.gov/cgi-bin/text-idx?SID=23094eb7dfd7c239453269a275e57bd9&mc=true&node=se14.3.139_1325&rgn=div8	Public
e-CFR Airport Security.	September 2019	Part 1542	e-CFR	https://www.ecfr.gov/cgi-bin/text-idx?SID=5a1b08bbf0c88da7072c6659eb56b91f&mc=true&node=pt49.9.1542&rgn=div5	Public
e-CFR Aviation and Transportation Security Act (ATSA). Public Law 107-71 49 CFR Subchapter C: Civil Aviation Security	September 2019	0.0	e-CFR	https://www.ecfr.gov/cgi-bin/text-idx?SID=64c8cd132dcd0e5ea413bb5c59dde720&mc=true&tpl=/ecfrbrowse/Title49/49CXIIsubchapC.tpl	Public
e-CFR Certification and Operations: Land Airports	September 2019	Part 139	e-CFR	https://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title14/14cfr139_main_02.tpl	Public
e-CFR Civil Aviation Security General Requirements	September 2019	Part 1540	e-CFR	https://www.ecfr.gov/cgi-bin/text-idx?SID=5a1b08bbf0c88da7072c6659eb56b91f&mc=true&node=pt49.9.1540&rgn=div5	Public
e-CFR Foreign Air Carrier Security	September 2019	Part 1546	e-CFR	https://www.ecfr.gov/cgi-bin/text-idx?SID=5a1b08bbf0c88da7072c6659eb56b91f&mc=true&node=pt49.9.1546&rgn=div5	Public
e-CFR Indirect Air Carrier Security	September 2019	Part 1548	e-CFR	https://www.ecfr.gov/cgi-bin/text-idx?SID=5a1b08bbf0c88da7072c6659eb56b91f&mc=true&node=pt49.9.1548&rgn=div5	Public
e-CFR Protection of Sensitive Security Information	September 2019	49 CFR § 1520	e-CFR	https://www.ecfr.gov/cgi-bin/text-idx?SID=5ddce3a9f2f522c0c5fa2e4b4ad3da23&mc=true&node=pt49.9.1520&rgn=div5	Public
Electronic Industry Alliance (EIA)			ECA	http://ec-central.org/index.cfm	Public
Ergonomic and workplace standards and requirements of the U.S. Department of Labor Occupational Safety & Health Administration (OSHA)				https://www.osha.gov/SLTC/etools/baggagehandling/index.html https://www.osha.gov/SLTC/ergonomics/ https://www.osha.gov/SLTC/etools/computerworkstations/components_monitors.html	Public

Document Name	Issue Date	Version	Issued By	Website	Availability
Existing and Potential Standoff Explosives Detection Techniques	2004		The National Academies Press	https://www.nap.edu/catalog/10998/existing-and-potential-standoff-explosives-detection-techniques	For Purchase
FAA Advisory Circular Checklist	July 2004	00.2-15	FAA	https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/74299	Public
FAA Airport Design	September 2012	150/530 0-13A	FAA	https://www.faa.gov/airports/resources/advisory_circulars/index.cfm/go/document.current/documentnumber/150_5300-13	Public
FAA Airport Emergency Plan	June 2009	AC 150/520 0-31C	FAA	https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/74488	Public
FAA Airport Terminal Planning	July 13, 2018	150/536 0-13A	FAA	https://www.faa.gov/airports/resources/advisory_circulars/index.cfm/go/document.current/documentNumber/150_5360-13	Public
FAA Foreign Air Carrier Security	June 10, 1982	AC 129-3	FAA	https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/22525	Public
FAA Standard Specifications for Construction of Airports	December 21, 2018	AC 150/537 0-10H	FAA	https://www.faa.gov/airports/resources/advisory_circulars/index.cfm/go/document.current/documentnumber/150_5370-10	Public
Federal Communication Commission (FCC)			FCC	https://www.fcc.gov/	Public
FEMA 426 Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings	December 2003		DHS/FEMA	https://www.fema.gov/media-library-data/20130726-1455-20490-6222/fema426.pdf	Public
FEMA 427 Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks	December 2003		DHS/FEMA	https://www.fema.gov/media-library-data/20130726-1455-20490-6114/fema427.pdf	Public
FEMA 452, A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings	January 2005		DHS/FEMA	https://www.fema.gov/media-library/assets/documents/4608	Public

Document Name	Issue Date	Version	Issued By	Website	Availability
FEMA 453 Safe Rooms and Shelters: Protecting People Against Terrorist Attacks	May 1, 2006		DHS/FEMA	https://www.fema.gov/media-library/assets/documents/4498	Public
FEMA 455 Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks	March 1, 2009		DHS/FEMA	https://www.fema.gov/media-library/assets/documents/2298	Public
FEMA 459 Incremental Protection for Existing Commercial Buildings from Terrorist Attack	April 2008		DHS/FEMA	https://www.fema.gov/media-library/assets/documents/13311	Public
FEMA National Incident Management System	October 2017	3rd Edition	FEMA	https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_2017.pdf	Public
Federal Inspection Services (FIS) Section 233(b) of the Immigration and Nationality Act (INA)			FIS	https://www.govinfo.gov/content/pkg/BILLS-114s1593is/html/BILLS-114s1593is.htm	Public
FIS Title 8 part 234, section 4 of the CFR: International Airports for Entry of Aliens	January 1, 2001		FIS	https://www.govinfo.gov/app/details/CFR-2001-title8-vol1/CFR-2001-title8-vol1-sec234-4	Public
General Services Administration Alternate Path Analysis & Design Guidelines for Progressive Collapse Resistance	January 28, 2016	Revision 1	GSA	https://www.gsa.gov/real-estate/design-construction/engineering-and-architecture/security-engineering/2016-alternate-path-analysis-design-guidelines-for-progressive-collapse-resistance	Public
Guidance for Planning, Design and Operations of Airport Communications Centers - Research Report 182	2018		ACRP	https://www.nap.edu/catalog/24980/guidance-for-planning-design-and-operations-of-airport-communications-centers	Public
Guidelines for Managing the Security of Mobile Devices in the Enterprise	June 2013	Revision 1	NIST	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf	Public
Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism	May 2005		BERKELEY LAB	https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2005/053237.pdf	Public
Homeland Security Act, Public Law 107-296	November 25, 2002	0	HSDL	https://www.hsdl.org/?abstract&did=614	Public

Document Name	Issue Date	Version	Issued By	Website	Availability
Homeland Security Affairs, Assessing Homeland Security Risks: A Comparative Risk Assessment of 10 Hazards			Homeland Security	https://www.hsaj.org/articles/7707	Public
Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors	August 19, 2015		Homeland Security	https://www.dhs.gov/homeland-security-presidential-directive-12	Public
IATA, The Airport Development Reference Manual (ADRM)	March 2019	Edition 11	IATA	https://www.iata.org/publications/store/Pages/airport-development-reference-manual.aspx	For Purchase
ICAO Airport Planning Manual—Master Planning, Part 1 (Doc 9184)	1987	2nd Edition	ICAO	https://www.icao.int/Pages/default.aspx	For Purchase
IEEE802, IEEE 802 LAN/MAN Standards Committee			IEEE	http://www.ieee802.org/	Public
Institute of Electrical and Electronic Engineers (IEEE)			IEEE	https://www.ieee.org/	Public
International Building Code Council			ICC	https://www.iccsafe.org/	Public
International Civil Aviation Organization—Standards and Recommended Practices—Security—Safeguarding International Civil Aviation Against Acts of Unlawful Interference	April 2017		ICAO	https://www.icao.int/Security/SFP/Pages/Annex17.aspx	For Purchase
International Standards and Recommended Practices—Security—Aerodromes—Annex 14	July 2013	Volume 1	ICAO	https://www.icao.int/Pages/default.aspx	For Purchase
International Telecommunications Union (ITU)				https://www.itu.int/en/Pages/default.aspx	Public
Internet Engineering Task Force (IETF)				https://www.ietf.org/	Public
Internet of Things (IoT): A vision, architectural elements, and future directions	September 2019		Future Generation Computer Systems	https://www.sciencedirect.com/science/article/abs/pii/S0167739X13000241	Public

Document Name	Issue Date	Version	Issued By	Website	Availability
Comparing Homeland Security Risks Using a Deliberative Risk Ranking Methodology	September 2013		RAND	https://www.rand.org/pubs/rgs_dissertations/RGSD319.html	Public
MASTERSPEC			CSI	https://www.csiresources.org/standards/masterformat	For Purchase
Merritt Risk Management Manual	2015		Silver Lake	http://www.silverlakepub.com/Merritt_Risk_Management_Manual.php	For Purchase
National Electric Code (NEC)			NEC	https://www.nfpa.org/NEC	For Purchase
National Emergency Number Association, NENA Master Glossary of 9-1-1 Terminology			NENA	https://www.nena.org/default.aspx	Public
National Fire Codes NFPA 101			NFPA	https://www.nfpa.org/	For Purchase
National Fire Codes NFPA 415			NFPA	https://www.nfpa.org/	For Purchase
National Safe Skies Alliance				https://www.sskies.org/	Public
National Transportation Safety Board			NTSB	https://www.nts.gov/Pages/default.aspx	Public
NIST 800-53 "controls"		Revision 4	NIST	https://nvd.nist.gov/800-53	Public
NIST Risk Management Framework (RMF)			NIST	https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview	Public
NISTIR 8053 De-Identification of Personal Information	October 2015	NISTIR 8053	NISTIR	https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf	Public
PARAS 0002 – Companion Design Guide to US Customs and Border Protection's Airport Technical Design Standards	May 2017		Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0002.CBPATDSCompanionGuide.FinalReport.pdf	Public
PARAS 0008 – Findings and Practices in Sharing Sensitive Information (Synthesis Report)	February 2017		Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0008.SharingSensitiveInfo.FinalReport.pdf	Public

Document Name	Issue Date	Version	Issued By	Website	Availability
PARAS 0014 – Blast Mitigation Strategies for Non-Secure Areas at Airports	August 2018		Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0014.BlastMitigationStrategies.FinalGuidebook.pdf	Public
PARAS 0007 – Quick Guide for Airport Cybersecurity	January 2018		Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0007.CybersecurityQuickGuide.FinalReport.pdf	Public
PARAS 0009 – Guidance for Security Management Systems	March 2018		Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0009SeMS_Guidance-Final.pdf	Public
PARAS 0010 – Guidance for Protecting Access to Vital Systems Impacting Airport Security	October 2017		Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0010.SecuritySystemsAccess.FinalReport.pdf	Public
PARAS 0015 – Guidance for Airport Perimeter Security	December 2018		Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0015.AirportPerimeterSecurity.FinalReport.pdf	Public
PARAS 0016 – Airport Security Vulnerability Assessments	June 2020		Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0016.SVAGuidebook_Final_.pdf	Public
PARAS 0017 – Access Control Card Technology Guidance	October 2019		Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0017_Access_Control_Card_Tech_Guidance.pdf	Public
PARAS 0023 – Exit Lane Strategies and Technology Applications	TBD		Safe Skies	https://www.sskies.org/paras/reports/	Public
Presidential Decision Directives				https://fas.org/irp/offdocs/direct.htm	Public
Privacy and Civil Liberties Interim Guidelines: Cybersecurity Information Sharing Act of 2015	February 2016		DHS	https://www.congress.gov/bill/114th-congress/senate-bill/754	Public
RTCA DO-2301 – Standards for Airport Security Access Control Systems	June 21, 2018		ACRP	https://www.rtca.org/content/sc-224-airport-security-access-control-systems-11	For Purchase
Secured Cities, May the Social Media Force Be With You	March 23, 2015		SIW	https://www.securityinfowatch.com/cybersecurity/information-security/article/12050427/social-reveals-both-sides-of-human-nature-when-it-comes-to-security	Public
Security 101: Physical and Cybersecurity Primer for Transportation Agencies	2019		ACRP	https://www.nap.edu/catalog/25554/security-101-a-physical-and-cybersecurity-primer-for-transportation-agencies	Public

Document Name	Issue Date	Version	Issued By	Website	Availability
Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference	2017	10th Edition	ICAO	https://www.icao.int/Security/SFP/Pages/SecurityManual.aspx	For Purchase
Social Media: Leveraging Value While Mitigating Risk	2013		NIST/HHS OCR	https://csrc.nist.gov/CSRC/media/Presentations/HIPAA-2013-Social-Media-Leveraging-Value-While/images-media/etue_day1_315_leveraging_social_media_while_mitigating_risk.pdf	Public
Standards for Airport Security Access Control Systems	2017	RTCA/D O-230G	RTCA	https://standards.globalspec.com/std/13051958/RTCA%20DO-230	For Purchase
Telecommunications Industry Association (TIA)				https://www.tiaonline.org/	Public
Terrorism in the United States—Terrorist Research and Analytical Center, Counter Terrorism Section, Criminal Investigative Division			FBI	https://www.fbi.gov/investigate/terrorism	Public
The Critical Infrastructure Key Resource (CIKR) Annex			DHS	https://www.cisa.gov/critical-infrastructure-and-key-resources-support-annex	Public
The Design and Evaluation of Physical Protection Systems	2001		Butterworth - Heinemann	Available for purchase at Internet book sites	For Purchase
The International Organization for Standardization (ISO)			ISO	https://www.iso.org/home.html	Public
The Internet of Things: Sizing up the opportunity	December 2014		McKinsey & Company	https://www.mckinsey.com/industries/semiconductors/our-insights/the-internet-of-things-sizing-up-the-opportunity	Public
Privacy Research and Best Practices: Summary of a Workshop for the Intelligence Community	2016		The National Academies Press	https://www.nap.edu/catalog/21879/privacy-research-and-best-practices-summary-of-a-workshop-for	Public
The Public Transportation System Security and Emergency Preparedness Planning Guide	January 2003	Final Version	DOT	https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/PlanningGuide.pdf	Public

Document Name	Issue Date	Version	Issued By	Website	Availability
The Risk Management Process for Federal Facilities: An Interagency Security Committee Standards	November 2016	2nd Edition	DHS	https://www.dhs.gov/publication/isc-risk-management-process	Public
TIA Administrative Standard for Telecommunications Infrastructure	June 2012	TIA-606-B	TIA	http://az776130.vo.msecnd.net/media/docs/default-source/contractors-and-bidders-library/standards-guidelines/it-standards/tia-606-b.pdf?sfvrsn=2	Public
Transit Security Design Considerations	November 2004	Final	DOT	https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/ftasesc.pdf	Public
TSA Checkpoint Design Guide (CDG)	June 1, 2016	Revision 6.1	TSA	http://files.constantcontact.com/8c363cd8001/f070043f-495f-42bf-99b4-d1688c57e199.pdf	Public
TSA Electronic Baggage Screening Program (EBSP)			TSA	https://www.tsa.gov/for-industry/electronic-baggage-screening	Public
TSA NEDCTP Canine Training & Evaluations Branch			TSA NEDCTP	https://www.dhs.gov/keywords/national-explosives-detection-canine-team-program	Public
TSA Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems (CBIS)	September 29, 2017		TSA	https://iabsc.org/pgds/	Public
TSA Planning Guidelines and Design Standards for Checked Baggage Inspection Systems	September 26, 2017	6.0	TSA	https://www.fbo.gov/spg/DHS/TSA/HQTSA/TSA25-04-03026/listing.html	Public
TSA Security Checkpoint Layout Design Reconfiguration Guide	November 7, 2006	Version 1	TSA	https://www.academia.edu/23029635/Checkpoint_Layout_Design_Guide_v1r0_0	Public
TSA Security Guidelines for General Aviation Airports. Aviation Security Advisory Committee	July 2017	Version 2	TSA	https://www.tsa.gov/sites/default/files/2017_ga_security_guidelines.pdf	Public
Americans with Disabilities Act (ADA) for regulatory requirements and guidance	September 15, 2010		DOJ	https://www.ada.gov/2010ADASTandards_index.htm	Public
UFC 3-340-02 Structures to Resist the Effects of Accidental Explosions, with Change 2	August 19, 2014	Change 2	DoD	https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-3-340-02	Public

Document Name	Issue Date	Version	Issued By	Website	Availability
UFC 4-010-01 DoD Minimum Antiterrorism Standards for Buildings	September 11, 2008		DoD	https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_01_2018.pdf	Public
UFC 4-020-01 DoD Security Engineering Facilities Planning Manual	September 11, 2008		DoD	https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-020-01	Public
UFC 4-022-02 Selection and Application of Vehicle Barriers, with Change 1	August 9, 2010	Change 1	DoD	https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-022-02	Public
UFC 4-023-03 Design of Buildings to Resist Progressive Collapse, with Change 3	November 1, 2016	Change 3	DoD	https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-023-03	Public
Unified Facilities Criteria (UFC), Emergency Operations Center Planning and Design	July 15, 2008		UFC	https://www.wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-141-04	Public
WBDG Glazing Hazard Mitigation	January 15, 2016		WBDG	http://www.wbdg.org/resources/glazing-hazard-mitigation	Public

APPENDIX C: AVIATION SECURITY BACKGROUND AND HISTORY

The Aviation Security Improvement Act of 1990²¹ directed the FAA to develop a guideline document for airport design and construction, to help ensure security enhancements and improvements are taken into account at the earliest stages of planning and design. This legislation was influenced by recommendations of the 1990 President's Commission on Aviation Security and Terrorism, which believed that the FAA should determine the security features necessary for new airport facilities and ensure that they are included in design and construction, recognizing that many airport structures at that time did not accommodate the application of appropriate security measures. The requirement for these guidelines was codified in 49 USC § 44914, and a later act added the requirement to consider the results of TVA performed under § 44904 when drafting these guidelines.

The Aviation and Transportation Security Act of 2001 (ATSA)²² created the TSA and passed the responsibility for developing these guidelines from FAA to TSA. The act authorizes increased federal responsibility for all aspects of aviation security, including federal assumption of passenger and baggage screening duties. The responsibilities of the TSA were defined further in 2002 with the passage of the Homeland Security Act²³, which created DHS. The primary missions of DHS include preventing terrorist attacks within the United States and minimizing the damage and assisting in the recovery from any attacks that may occur. DHS's primary responsibilities correspond to five major functions established by the Homeland Security Act: information analysis and infrastructure protection; chemical, biological, radiological, nuclear, and related countermeasures; border and transportation security; emergency preparedness and response; and coordination with other parts of the federal government, state and local governments, and the private sector.

Laws, regulations and official guidance in reports and audits provide information and justification for security-related construction and refurbishment at airports. They influence the content of the recommended security guidelines and their use by airport operators. Consulting these documents will give airport management and affected parties insight into current and future requirements, and planned government actions. Newly available technological tools for TVA, risk management, flow modeling, and blast protection can reduce guesswork and minimize certain expenditures for security enhancements and improvements in new airport facilities and structures.

For example, the Department of Homeland Security Appropriations Act of 2015²⁴ appropriated funds for TSA civil aviation security services provided that “any award to deploy explosives detection systems shall be based on risk, the airport's current reliance on other screening solutions, lobby congestion resulting in increased security concerns, high injury rates, airport readiness, and increased cost effectiveness.” These recommended security guidelines will be useful to airport operators during EDS installation planning with TSA. The act also provided funding established by 49 USC § 44923 for grants to airport operators for security improvement projects, including EDS-related baggage conveyor systems, terminal baggage area and ticket counter reconfiguration, and other airport security capital improvement projects. Note that § 556 of the act prohibits funds from being used by TSA to “implement, administer, or enforce... any requirement that airport operators provide airport-financed staffing to monitor exit points from the Sterile Area of any airport” at which TSA provided monitoring

²¹ Public Law 101–604: <https://www.govinfo.gov/content/pkg/STATUTE-104/pdf/STATUTE-104-Pg3066.pdf>

²² Public Law 107–71: <https://www.govinfo.gov/content/pkg/PLAW-107publ71/pdf/PLAW-107publ71.pdf>

²³ Public Law 107–296: <https://www.govinfo.gov/content/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf>

²⁴ Public Law 114–4: <https://www.congress.gov/114/plaws/publ4/PLAW-114publ4.pdf>

in 2013.²⁵ The Transportation Security Acquisition Reform Act of 2014²⁶, required TSA to develop a five-year strategic plan for security technology investment and deployment that covers FY2016–2020. To mitigate the impact on airport operations, the law also requires TSA to consult with airport operators when an acquisition will cause the removal of installed TSA security equipment.

Most recently, House Resolution 302, known as the FAA Reauthorization Act of 2018, to strengthened aviation security by both clarifying the FAA/TSA mission and funding and expanding the future direction of aviation security. Key focal points of this Act relevant to airport security include FAA funding program/grant clarification and expansion, security technology use and approval updates, public area security studies and requirements, and various other topics addressing current and future security trends such as unmanned aircraft and passenger queue monitoring.

²⁵ See also Congressional Research Service DHS Appropriations Report R43796

²⁶ Public Law 113–245: <https://www.govinfo.gov/content/pkg/PLAW-113publ245/pdf/PLAW-113publ245.pdf>

APPENDIX D: GENERAL AVIATION

Recommendations in this section are tailored for GA operating areas located at airports with commercial service regulated under CFR § 1542, as well as airports serving only GA aircraft.

Operational recommendations, such as establishing a community watch program and the use of auxiliary aircraft locking devices, may also be found through guidance published by the Aircraft Owners and Pilots Association (AOPA).

INTRODUCTION

GA refers to all aviation except scheduled commercial passenger airlines and the military. The approximately 225,000 GA aircraft constitute about 75 percent of all air traffic in the United States. GA operations are different from commercial operations in that passengers of GA aircraft do not undergo screening, except under certain limited conditions. Passengers aboard the GA aircraft are typically known by the pilot in command, who has final authority over what items may be carried onboard the aircraft.

GA operations at commercial service airports should be evaluated, designed, and located independently from commercial operations areas as much as is practicable, so as to minimize potential security conflicts, flight delays, and unnecessary inconveniences to both GA and commercial service operators. Imposing commercial designs and procedures on GA may result in unnecessary restrictions, potentially causing a decline in operations at the airport and a drop in GA activity and revenues.

SECURITY AREAS AND BOUNDARIES

In general, it is advisable that GA operations are excluded from operating in the SIDA of the airport as much as is practicable. If this is not possible, operational limits should be considered to eliminate any possible breach of § 1542 security requirements. GA passengers, crews, cargo, and baggage should be screened when entering Sterile Areas; or alternatively, these items should proceed through clearly marked and controlled areas away from Sterile Areas.

- At commercial service airports where the AOA precludes separate fencing or barriers for the GA aircraft operating area, clear signage and ground markings are important to prevent GA operators from inadvertently crossing into SIDA or Sterile Areas of the tarmac, triggering a security response.
- When addressing security controls of GA operations and persons at commercial airports, the principle to be followed is that of complete separation from commercial traffic. Separation is normally accomplished by designing GA aircraft parking areas that lie outside of areas secured for commercial operations, often on the opposite side of the airport.
- Ramp parking arrangements should be designed to ensure visual observation of aircraft and passengers during the embarking and disembarking process.

RAMP SECURITY MEASURES

FBO/GA terminal operators should consider the design of secure or monitored access doors and gates for each portal leading to the aircraft ramp. They should provide signage that clearly restricts access to the AOA to authorized persons only. Depending on individual airport security procedures and location on the field, the FBO doors may be included on the airport access control system.

SIGNAGE

The use of signage provides a deterrent by warning of facility boundaries, as well as notifying individuals of the consequences of a violation. Signs should be constructed of durable materials, contrasting colors, and reflective material where appropriate. Use of concise and consistent language is recommended.

Wording may include, but is not limited to, warnings against trespassing, unauthorized use of aircraft and tampering with aircraft, and reporting of suspicious activity (e.g., AOPA's Airport Watch [Figure 24] and "See Something, Say Something.") Signage should include phone numbers of the nearest responding law enforcement agency, 9-1-1, and/or TSA's 1-866-GA-SECUR, as appropriate.

LIGHTING AND CAMERAS

FBO and terminal operators should consider outdoor security lighting and cameras to improve the security of:

- Aircraft parking and hangar areas
- Fuel storage areas and fuel trucks
- Airport access control points, including at the perimeter
- Other appropriate areas, such as vehicle parking, fences, or obstructed areas

BASED AIRCRAFT

Facility planners should consider design elements that will allow home-based GA operators to access their aircraft when the FBO is closed, such as combination locks at pedestrian gates or key code access. Depending on airport security requirements and AOA configuration, airport ID badging might be required.

BUILDING DESIGN FACTORS

Design should maximize visibility between the line office and transient and home-based tie-down areas.

- The customer service/reception area should have a clear view of all doorways and other access points leading to the ramp.
- Hangar access should be controlled and restricted to authorized personnel only. In some circumstances, the GA area access controls may be tied to the airport ACS. Ramp access from the FBO or terminal should be controlled and restricted to authorized personnel only.
- Vehicle access, including pilot, passenger, taxi, livery, or delivery access to the ramp should be monitored via CCTV or visual inspection to establish a positive identification prior to operating the gate access control to the ramp. The driver can be separated from the vehicle if necessary to ensure the driver is not under duress.
- Planners should consider minimizing ramp access by all vehicles as much as possible.

INTERNATIONAL GENERAL AVIATION

Where possible, the design of separate CBP or FIS facilities should be incorporated using the CBP Airport Technical Design Standards.

Figure 24. AOPA Airport Watch Signage



Source: AOPA

Reference and Guidance Documents

For additional guidance on General Aviation Security Guidelines, refer to [TSA Security Guidelines for General Aviation Operators and Users](#).²⁷

For preclearance procedures for airport GA facilities, refer to [CBP Preclearance of General Aviation Summary Guide](#).²⁸

²⁷ For download: https://www.tsa.gov/sites/default/files/2017_ga_security_guidelines.pdf

²⁸ For download: https://www.cbp.gov/sites/default/files/documents/CBP_Preclearance_of_General_Aviation_Summary_Guide.pdf

APPENDIX E: INTERNATIONAL AVIATION SECURITY

Planning Requirements

CBP publishes an *Airport Technical Design Standard* (ATDS) that reflects national policy, procedures, and facility development standards for the design and construction of CBP facilities at U.S. airports and foreign preclearance facilities.

CBP MISSION REQUIREMENTS

In accordance with CBP's mission to secure the nation's borders while facilitating trade and travel, CBP processes and controls inbound international traffic to ensure persons, baggage, and cargo are not concealing illegal substances, contraband, or threats to national security. In support of its mission, CBP has established unified primary inspection processes at all United States ports of entry, along with specialized secondary inspections focused on combating terrorism. CBP implements various technologies, equipment, and processes to facilitate passenger processing. The airport operator is required to provide the space and infrastructure to support these measures. CBP will provide related information at the start of the design process to minimize impacts during construction. CBP also facilitates the work of other government agencies, including the CDC, among others, in the clearance of goods and people.

ROLE OF AIRPORT TECHNICAL DESIGN STANDARD

CBP's ATDS was last published in 2017 and includes specifications for size of the facility based on the number of peak hour inbound passengers, as well as requirements for security and process flows for passengers and checked bags.

The document also discusses passenger and baggage flow, terminal building space utilization, as well as offices, processing booths, counters, conveyors, x-ray systems, access control, and other equipment necessary to support the monitoring, control, and operation of the FIS facility.

While preparing a design for an airport project, refer to the most current CBP standards when accommodating the agency's requirements.

RECENT PROCESS CHANGES

CBP is undertaking a major effort to reduce the amount of manual work for CBP officers and increase automation and partnerships with airlines/airports. Some results include:

- Automated Passport Control kiosks to reduce wait-time for CBP processing
- Mobile Passport Control to enable eligible passengers with a smartphone to answer questions in-flight before landing
- Expansion of Global Entry, with full access to TSA Pre✓™ lanes
- Baggage-First/Consolidated Primary

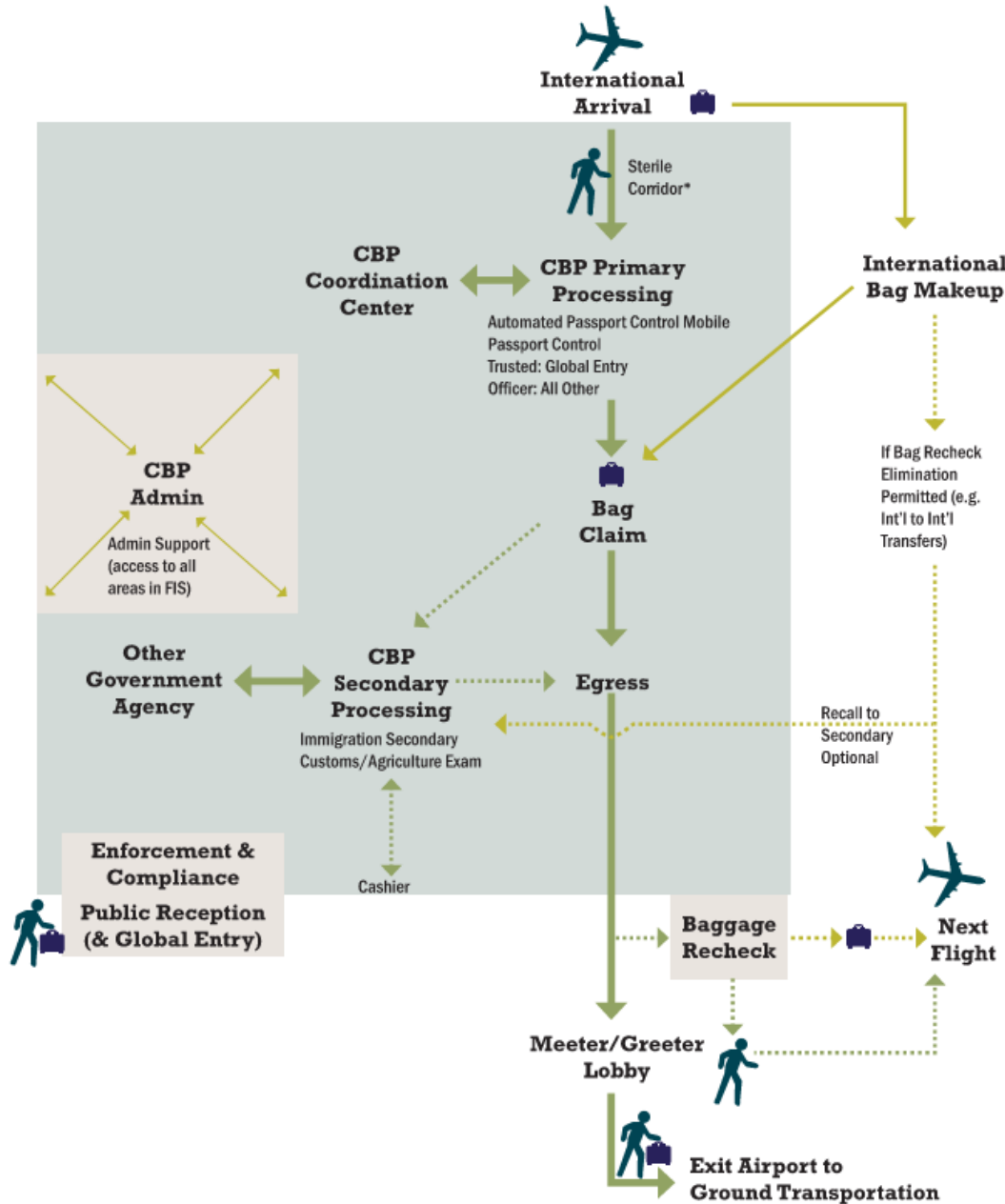
For regular operations at most CBP facilities, passenger flows are similar to the 2011 set of processes where, as shown in Figure 25, an international arrivals proceed directly to CBP primary processing. There are now also a range of automated processes (e.g., Automated Passport Control, Global Entry, mobile passport) before a passenger proceeds to bag claim.

From bag claim, a passenger can proceed to leave the facility through CBP Egress into the public area.

As noted in recent years, a number of connecting hubs have moved away from baggage recheck for certain flights. In this case, the diagram allows for international-to-international transfers, unless CBP has recalled a bag for secondary review. Passengers proceed to be screened by TSA prior to proceeding to their next flight.

Figure 25. International Arrivals: Bag Claim after Primary

International Arrivals: Bag Claim After Primary



* CDC may have a role occasionally to screen/monitor travellers (e.g., Ebola)

Major Facility Changes

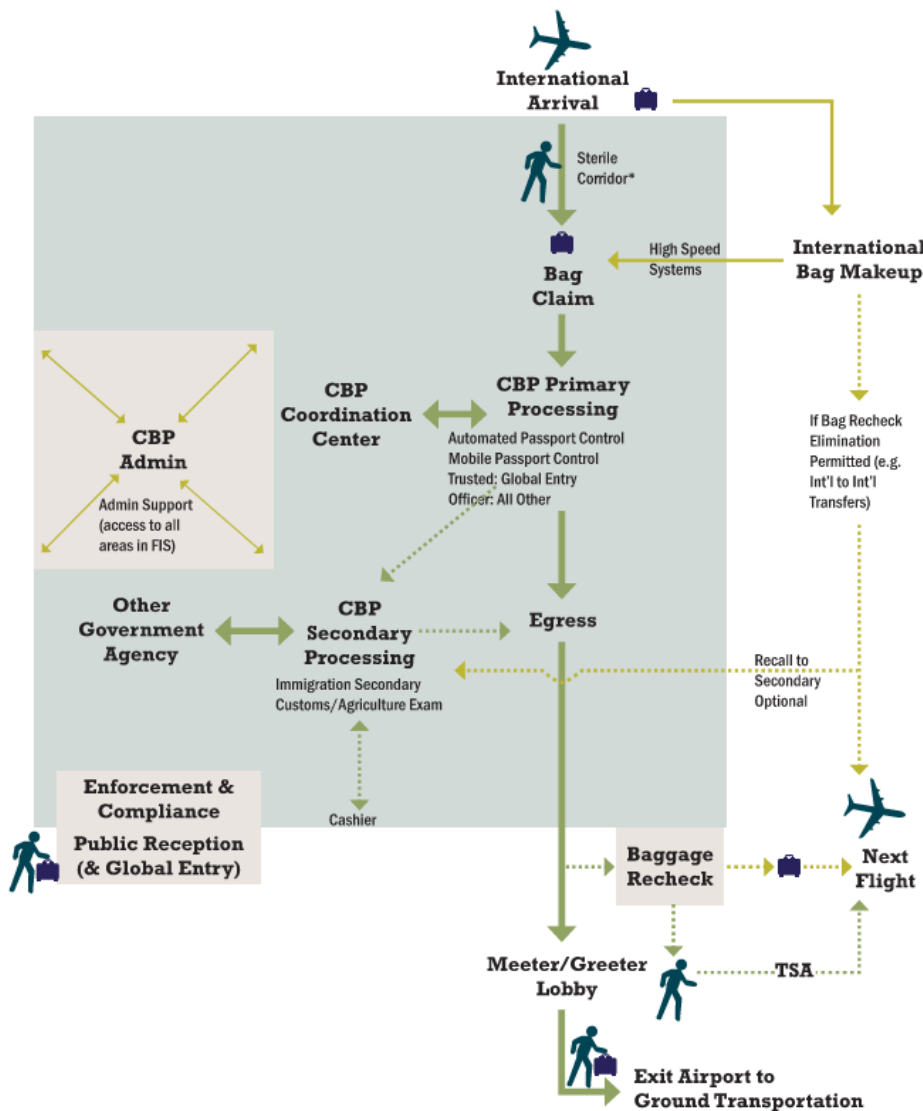
BAGS FIRST

Legacy agencies (Customs, Immigration & Naturalization Service) created primary secondary processing in 1971 to address international passenger volumes. Most facilities built after this time were created to allow bag claim after primary processing (passport check, biometric for foreign nationals, declaration). The ATDS has held to the separation of functions for primary and secondary.

CBP has modified the passenger processing procedures from a two-step inspection process to a single step defined as Consolidated Primary. With Consolidated Primary, the processing approach of Bag First was also implemented. Under this process, all passengers pick up bags first, before proceeding to see a CBP officer. There are implications for baggage security with the changes in bag flows and their proximity to recheck/re-screening devices. The optional process flows are shown in Figure 26.

Figure 26. International Arrivals Bags First before Primary

International Arrivals: Bags First Before Primary



* CDC may have a role occasionally to screen/monitor travellers (e.g., Ebola)

PRECLEARANCE EXPANSION

CBP processed approximately 137 million international passengers in FY 2019. In 2020, there were 16 preclearance sites around the world performing full CBP clearances in Canada, The Caribbean, Ireland, and Abu Dhabi. In 2015, 11 new sites were announced for consideration, including Amsterdam Schiphol; Punta Cana, Dominican Republic; Stockholm, Sweden; Manchester, England; and Tokyo Narita, among others. Also in 2015, CBP also issued a second call for proposals for new sites. Several will be opened in the coming years to start the process of moving border clearances away from the United States.

CBP has a stated goal to reach 33% of passengers pre-cleared by 2025—almost double what was observed in FY 2019. This will have several implications for US airports and CBP facilities:

- Elimination of TSA rescreening for precleared passengers and bags, provided TSA standards for screening are met. Similar to arrangements from precleared airports in Canada, if equipment and processes are deemed equivalent, there is no need for TSA rescreening for passengers connecting to an international or domestic flight.
- Shared baggage facilities: Most domestic US airports are not planned for large numbers of gates that accommodate large aircraft (e.g. A380). New preclearance flights could prompt the demand for large aircraft gates for domestic facilities. An alternate process could see the international claim devices within a CBP area with a temporary partition to allow for domestic operations.

Reference and Guidance Documents

Additional guidance on CBP facility security requirements, refer to US CBP Airport Technical Design Standard.

The companion to this document is Sake Skies [PARAS0002 – Companion Design Guide to US Customs and Border Protection’s Airport Technical Design Standards](#).²⁹

²⁹ For download: https://www.sskies.org/images/uploads/subpage/PARAS_0002.CBPATDSCompanionGuide.FinalReport.pdf

APPENDIX F: ALTERNATE TVA METHODOLOGIES

RISK ANALYSIS AND MANAGEMENT FOR CRITICAL ASSET PROTECTION (RAMCAP)

RAMCAP is a framework for analyzing and managing the risks associated with terrorist attacks against critical infrastructure assets. RAMCAP provides a consistent and technically sound methodology to identify, analyze, quantify, and communicate the various characteristics and impacts that may lead terrorists to select a particular target, and the impacts from a specific form of attack. It documents a process for identifying security vulnerabilities and provides methods to evaluate the options for improving these weaknesses.

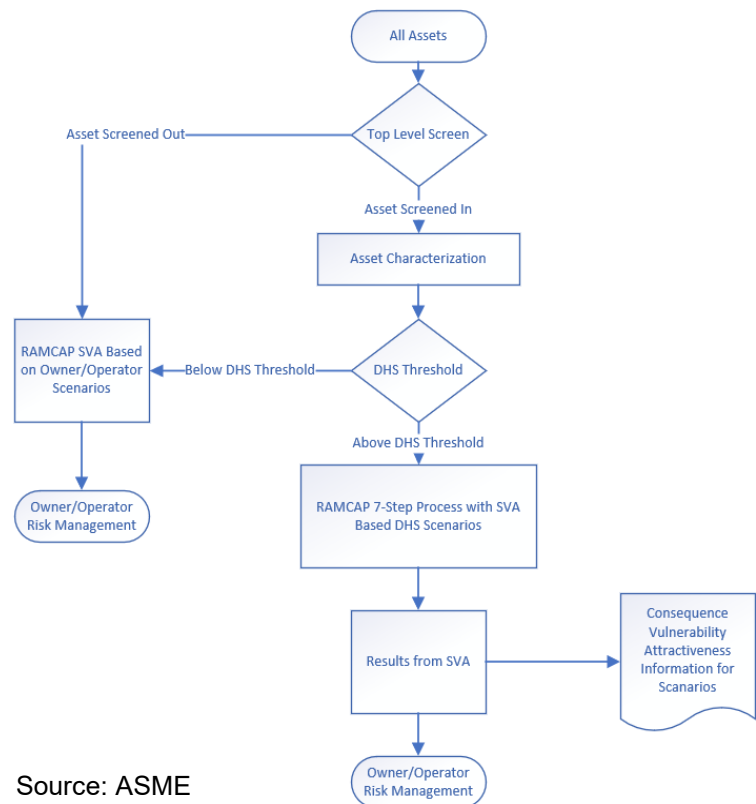
RAMCAP was developed with four major objectives in mind:

1. Define a common framework that can be used by owners and operators of critical infrastructure to assess the consequences and vulnerabilities relating to terrorist attacks on their assets and systems
2. Provide guidance on methods that can be used to assess and evaluate risk through the use of this common framework, which is illustrated in Figure 27.
3. Provide an efficient and consistent mechanism that can be applied to diverse elements of both private and government (Federal, State, and local) sectors to report essential risk information to DHS, which is crucial to the execution of responsibilities assigned to DHS
4. Identify which assets will be analyzed under the RAMCAP process based on DHS risk threshold

RAMCAP comprises seven steps:³⁰

1. Asset characterization and screening is the analysis of a facility or system's operational processes to identify critical assets and hazards, while making a preliminary forecast of potential consequences from a terrorist act. The assets evaluated include both physical and cyber assets. The analysis includes identification of existing layers of protection.
2. Threat characterization is the identification of specific and general modes of attack that may be used by terrorists against a given target. DHS has developed a set of baseline threats that are to be evaluated for each asset or system, based on the collective activities of law enforcement and intelligence organizations that are charged with developing an understanding of the means, methods, and motivations of terrorists. The threats include various modes of attack (e.g., air,

Figure 27. RAMCAP Process Flow Diagram



Source: ASME

³⁰ <https://files.asme.org/ASMEITI/RAMCAP/12604.pdf>

land, and water), and various sizes of attack (e.g., small, medium, large). The owner/operator then applies these threats to the facility or system based on in-depth knowledge of the operation's assets. Not all threats apply to all assets, so some threats will be screened from further consideration.

3. Consequence analysis is the identification of the worst reasonable consequences that could be generated by the specific threat. This step looks at facility or system design, layout, and operation in order to identify the types of consequences that might result. Consequences that are quantified include financial costs, fatalities, and injuries. Consequences that are noted qualitatively are psychological impacts and effects on national security or government functions.
4. Vulnerability analysis is the determination of the likelihood for a successful attack using a specific threat on a particular asset. This involves analyzing the existing security capabilities, countermeasures and mitigation strategies and their effectiveness in reducing the probability of a successful attack.
5. Threat assessment includes two steps: an evaluation of asset attractiveness and a full threat assessment. Asset assessment considers the perceived value to the terrorist of attacking a given facility or system considering the deterrence value of security measures and the robustness of the potential target. This area is assessed by the owner/operator. Threat assessment is performed by DHS and includes normalized assessments of attractiveness in light of the high-level objectives of terrorists and intelligence-based assessments of adversary capabilities and intent.
6. Risk assessment is a systematic and comprehensive evaluation of the previously developed terrorism-related data for a given facility or system. The owner/operator risk assessment creates a foundation for selecting strategies and tactics to defend against terrorist attacks by establishing priorities based on risk.
7. Risk management is the process of understanding risk and deciding upon and implementing action (e.g., defining security countermeasures, consequence mitigation features, or characteristics of the asset) to achieve an acceptable level of risk at an acceptable cost. Risk management is characterized by the identification, evaluation, and control of risks to a level commensurate with an assigned or accepted value.

FULL-SCALE SANDIA PROCESS³¹

The Full-Scale Sandia Process utilizes extensively researched quantitative risk data calculations for every threat, which makes it both highly precise and very costly to perform. This process is usually performed only by Sandia National Laboratories due to the expertise required to accommodate its stringent requirements successfully. It is outside the abilities of all but the most capable and well-equipped risk laboratory teams. This approach is highly recommended for high-consequence critical infrastructure facilities.

- Extremely robust analysis method
- Very scalable
- Completely scientifically supportable
- May be used qualitatively, quantitatively, or a combination of both
- Ideal for facilities where a very robust analysis is required necessitating very deep analysis of vulnerabilities, though can be used in a less robust fashion

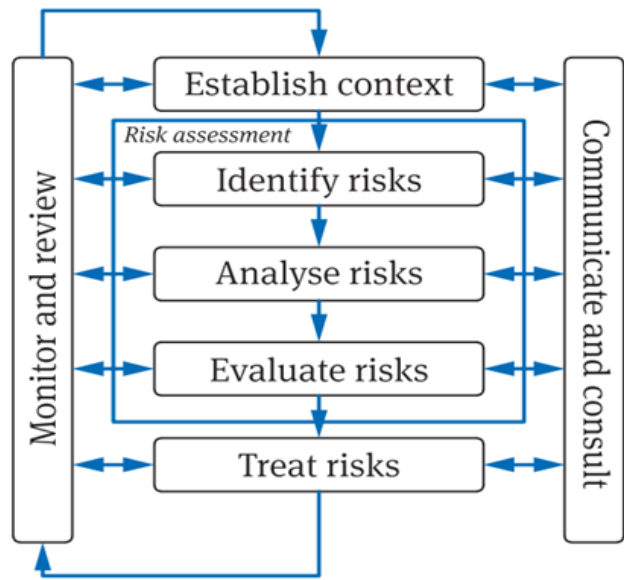
³¹ Norman, Thomas. (2015). *Risk Analysis and Security Countermeasure Process*

ISO 31000:2018 (ENTERPRISE SECURITY RISK MANAGEMENT – ESRM)

This methodology utilizes an internationally recognized standard that simplifies the risk assessment process and allows for flexibility when interpreting threats and risk. This process is descriptive, supporting better integration with the Owner’s overall enterprise risk management program. It describes risk management principles and the elements of a framework in general terms, and is adaptable to varying organizations, contexts, statutes, and environments.

This is a multi-step framework approach for organizations of all types and sizes that face internal and external influencers. The overall process is cyclical, identifies risks at all levels, and establishes an approach to document, communicate and monitor impacts to implemented mitigation solutions.

Figure 28. ISO 31000 Risk Management Process



Source: International Organization for Standardization

APPENDIX G: SECURITY SYSTEMS

Physical Security

TIME AND DISTANCE

Time and distance from critical facilities to be protected is a deterrent factor. If an unauthorized entry were to occur at a particular location, increasing the amount of time needed to cover the distance to the critical facility, combined with a high level of visibility, would significantly reduce the likelihood of the intruder reaching the target without detection and/or intervention. Time and distance may be considered an enhancement to standard physical barriers/boundaries when those boundaries are relatively removed from the critical areas they are protecting.

A remote area may require only moderate boundary security measures if it is sufficiently removed from the primary security-related areas, to allow the a PIDS time to detect an intrusion, and to delay the progress of the intruder until an appropriate security response can be implemented.

NATURAL BARRIERS

The use of natural barriers may be necessary at an airport in areas that cannot structurally support physical barriers or fencing, or where the use of fencing or physical barriers would cause conflict with aircraft navigation, communications, or runway clear areas beneath approach paths. With TSA approval, natural barriers may be incorporated into the security boundary of an airport as a complement to additional security measures or procedures. Natural barriers may include bodies of water, expanses of trees, swampland, dense foliage, cliffs, etc.

When considering whether a natural barrier is an appropriate boundary, the airport operator should take into account the findings of the TVA prepared for the airport PDD and whether the natural barrier should be complemented with other types of boundary protection. As noted previously, special attention should be given to areas where large bodies of water are used as public recreational or fishing areas near the airport boundary.

Earthen material may also be used to create a visual barrier between any public road and the AOA. This can be accomplished through various methods, such as trenching or stockpiling. Trenching may be done below the grade of any adjacent airfield surface, such as the perimeter road, and at a slope that would prevent an individual from acquiring a visual reference of the airfield. It is in the interest of the airport operator to have an above-grade barrier on the airport property for ease of maintenance and control. A fence may be constructed atop the barrier.

When considering the integration of Natural Barriers, [Crime Prevention Through Environmental Design](#)³² concepts would be considered and incorporated.


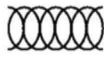


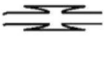


FENCES

Physical barriers can be used to deter and delay the access of unauthorized persons into nonpublic areas of airports. These are usually permanent and designed to be obvious visual barriers and physical obstacles. They also serve to meet safety requirements in many cases. Where possible, security fencing or other physical barriers should be aligned with security area boundaries, some of which may also require clear zones on one or both sides.

³² For download: <https://www.wbdg.org/resources/crime-prevention-environmental-design>

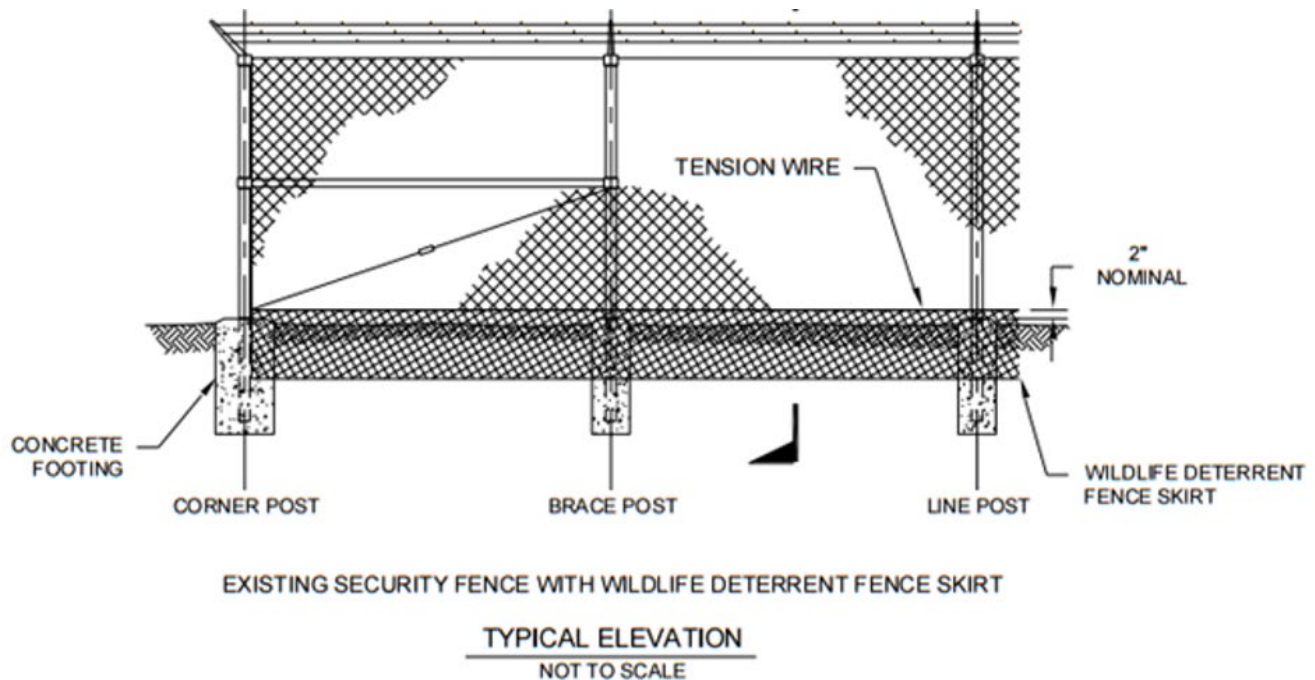
Fencing is available in several designs that are difficult to climb or cut. Figure 29 shows some of the available types of fence fabrics with American Iron and Steel Institute (AISI) and ASTM ratings.

Figure 29. Typical Chain Link Fence Barbed Wire Configurations

	PRODUCT	APPLICATION	SIZES	WT / ROLL	MATERIAL	ATTACHMENT SPACING LENGTH	BREAK LOAD
	RAZOR RIBBON— Single coil with core wire	Medium security fence topping	18" 24" 30"	13 lbs. 17 lbs. 21 lbs.	AISI 430 Stainless steel .098 dia. high Tensile wire	6"—16.6' 9"—2'5" 18"—5'0"	2800 lbs.
	RAZOR RIBBON— single coil with wire concertina style	Ground barrier Max. security fence topping	24" 30" 36"	15 lbs. 19 lbs. 23 lbs.	AISI 430 Stainless steel .098 dia. high Tensile wire	12"—1'5" 16"—2'0"	2800 lbs.
	RAZOR RIBBON MAZE— Concertina style, double coil	Ground barrier Max. security fence topping	24" inside 30" outside	34 lbs.	AISI 430 Stainless steel .098 dia. high Tensile wire	12"—1'5" 16"—2'0"	2800 lbs.
	MIL-B-52775 B Type II austenitic double coil	Ground barrier Max. security fence topping	24" inside 30" outside	35 lbs.	AISI 301/304 stainless steel .047 dia. stainless wire rope	24"—6'6"	2250 lbs.
	MIL-B-52775 B Type IV austenitic double coil	Ground barrier Max. security fence topping	24" inside 30" outside	35 lbs.	AISI 316 Stainless steel .047 dia. stainless wire rope	12"—1'5" 16"—2'0"	2250 lbs.
	RAZOR RIBBON— single coil	Min. security fence topping. Commercial use.	18" 24"	9 lbs. 12 lbs.	AISI 430 Stainless steel	6"—16.6' 9"—2'5" 18"—5'0"	1260 lbs.
	BAYONET BARB— Concertina	Ground barrier	27½" 37½"	23 lbs. 34 lbs.	ASTM A 526 Zinc galvanized .098 dia. high Tensile wire	20"—5'0"	1300 lbs.

Source: American Iron and Steel Institute

Chain link fencing is the most common type of fencing, and is often the most cost-effective solution when deterrence, as opposed to the prevention of forced entry, is the primary security objective. Chain link fences are typically constructed with seven feet of metal fabric plus three strands of barbed wire on top, angled outward at a 45-degree incline from the airside. Fabric should be secured to the fence posts in a manner that makes it difficult to loosen the fabric. Fabrics should also be buried at a depth that prevents intruders from lifting the fabric and crawling under it. A fence configured in this manner is shown in Figure 30. Use of concrete mow strips below the fence line can also deter tunneling underneath the fence by persons and animals. Mowing strips may also reduce maintenance hours and costs.

Figure 30. Security Fence with Wildlife Deterrent Fence Skirt

Chain link fencing is normally the most suitable and economical physical barrier for securing the airside, although this may vary somewhat with airport-specific conditions and topography. It is also readily available through a large variety of sources and is easily and inexpensively maintained. This type of fence provides clear visibility for security patrols and is available in varieties that can be installed in almost any environment. Barbed wire, razor wire, and other available toppings increase intrusion difficulty. For locations with aesthetic concerns, there are also a large variety of decorative yet functional styles available, as well as opaque styles that limit public visibility of service, storage, or other non-aesthetic areas.

When utilizing fencing as a security boundary, care should be taken to ensure that the fencing does not conflict with the operational requirements of the airport. Access points should permit passage of authorized vehicles and persons with relative ease. While the number of access points should be kept to a minimum, adequate access points should be planned for routine, maintenance, and emergency operations.

To assist in surveillance and security patrol inspection, fences should be as straight and uncomplicated as possible. This will minimize installation and maintenance costs not only for the fence itself, but for video surveillance lines of sight and detection zones for various sensors.

Fences can be provided with motion, tension, or other electronic sensing means. For fences with sensors, either mounted on the fencing or covering areas behind the fencing, other security system elements are needed to monitor the sensors and respond to intrusion alarms.

Wind is often an issue when designing chain link fencing to be instrumented with intrusion detection sensors, including wind-induced fence motion caused by proximity of fencing to runways and run-up areas or blast fences. Taut fence fabric is often required under such circumstances.

BUILDINGS AND WALLS

Buildings and other fixed structures may be used as a part of the physical perimeter barrier. They can be incorporated into a fence line if access control or other measures to restrict unauthorized passage

through the buildings or structures are taken at all points of access. Whether those points are located on the airside or landside boundaries, or through the middle of such buildings, may depend on the nature of the business being conducted inside and the level of continuous access required by personnel. Building design should ensure that fire escapes, maintenance access ladders, and utility tunnels do not provide an unobstructed path from the public side to airside.

Walls are one of the most common types of physical barriers. Various types of walls are used for interior as well as exterior security boundary delineation. They play an important part as visual barriers and deterrents.

VEHICLE BARRIERS

A vehicle barrier system must effectively stop and/or disable vehicles that pose a threat to the airport. Types of vehicle barriers include passive (static or removable) fixed perimeter barriers to active (operations for access control) barrier/wedges. They provide a physical barrier between vehicle traffic lanes and sensitive areas, and are also used to enforce a stand-off distance from an asset based on the outcome of the blast and risk assessments.

Barrier rating selection is based on the weight, speed, and angle of attack of the threat vehicle.

The previous Department of State performance requirements for vehicle crash barriers were based on the kinetic energy represented by the mass of a vehicle and its impact velocity. These “K” ratings were K4, K8 and K12, representing a 15,000-lb vehicle impacting at 30 mph, 40 mph, and 50 mph, respectively. The State Department stopped issuing these certifications in 2009. Testing and certification of perimeter barrier products is now carried out under ASTM F2656-16 *Standard Test Method for Vehicle Crash Testing of Perimeter Barriers*³³. This standard provides a wider range of criteria (vehicle size/weight, vehicle speed, vehicle penetration) with four choices of vehicle weights (2,430 lb, 5,070 lb, 15,000 lb, and 65,000 lb) moving at speeds of 30 mph, 50 mph, and 60 mph. Additionally, the rating system takes into account vehicle penetrations ranging from less than 1 meter to 30 meters or greater.

For older systems, the earlier ratings of K4, K8, and K12 are equivalent to the following ASTM system ratings:

- K4 = M30-P1
- K8 = M40-P1
- K12 = M50-P1

In the above ASTM ratings, M (mass) refers to the test vehicle weight of 15,000 lb, the 30, 40, and 50 refer to the nominal impact velocity of the vehicle, and P1 refers to penetration of less than 1 meter.

VEHICLE GATES

Typically, there are numerous access points through fencing or other barriers for both vehicles and pedestrians. Access points through buildings or walls are usually doors, though guard stations or electronic means or controls may be also used. In all cases, the access point type and design may determine the effectiveness of the security boundary and control in that area. Hence, in all cases, the number of access points should be minimized, and their use and conditions closely monitored.

Most airport gates are used for three categories of operations: routine, maintenance, and emergency.

³³ For purchase: <https://www.astm.org/Standards/F2656.htm>

Routine operations are generally high throughput and should be designed for high activity and long life. These gates will take the most wear and tear, and should be designed to minimize delays to users, particularly where piggybacking may be a concern. SIDA, Secured Area, AOA, and other security boundary gates that are high throughput are the most likely candidates for automation and electronic access control, and in some cases, manned guard posts.

Maintenance gates at an airport are those used by the airport, tenants, and FAA personnel to perform regular maintenance to remote grounds or equipment. Typical maintenance tasks include mowing, utility service, and upkeep on navigational and communications equipment. These gates, unless high-throughput or jointly used for routine operations, are usually non-automated and non-electronic.

Vehicle gates may also be used for emergency operations by on-airport and mutual-aid emergency response vehicles when responding to emergency situations. Additional (remote) control of these gates may occur from an airport operations center or from the ARFF response vehicles themselves to provide immediate access.

Gates should be constructed and installed to the same or greater standard of security as any adjacent fencing to maintain the integrity of the area.

All gates should be equipped to securely close and lock when authorized access of egress is not required. Swing gate hinges should be of the non-liftoff type or provided with additional welding to prevent the gates from being removed. Gate motor operator/controllers should be located on the secure side of the gate. Battery/UPS backup power for the gate operator motor and security devices (card readers, video surveillance cameras, buried induction loops, intercom, and area security lighting) to allow a 2-hour gate open-close operation is essential to continuing vehicle traffic circulation during a power failure.

Specifications should be based on the TVA mitigation recommendations for operational gate requirements. This should address dimensions, impact resistance, opening and closing times (especially important for gates controlling access to Secured Areas of the airport), direct and/or remote control, and integration with other security measures, including video surveillance of gate areas and their approaches, and possible vehicle-tracking measures.

A security gate's level of protection can be increased if they are designed and installed with no more than 4–6 inches of ground clearance beneath the gate. Where cantilever (slide) and/or rolling gates are used, consideration should be made during planning and design to accommodate curb heights, wheel paths, potential obstructions, local weather/wind, and drainage issues throughout the full path of the gate and adjacent areas. Proper drainage grading, planned gaps in curbs, installation of concrete channels or mow strips below the gate path, and use of bollards to prevent obstructions within the gate path and protect gate equipment are all design considerations that may prolong the efficient operation of a slide gate.

If tailgating entry is a concern at unstaffed vehicle access points, the first response is usually procedural rather than design, since it is the responsibility of the person authorized to use the gate to ensure that tailgating does not occur. However, if a fence design solution is desired, an automated two-gate system (also known as a sally port or vehicle entrapment gate) is one method that could help prevent tailgate entry. Such gates are separated slightly more than one vehicle length apart, and are sequenced so that the second gate does not open until the first has fully closed. Time-delayed closures are a viable alternative; sensor arrays can be used to monitor vehicle movement and assist in detection of tailgate entries. Tailgating and reverse tailgating (where a vehicle enters a gate that has been opened by an exiting vehicle) at automated gates may also be reduced by a security equipment layout that provides space for waiting vehicles to stop, which obstructs or at least deters other vehicles from passing through the gate. Video surveillance may deter breaches at those facilities and may provide an improved response when

breaches occur. Additionally, surveillance cameras may provide a visual record of breaches to be used in potential investigations. At unmanned gates, an open vehicle gate could be breached relatively easily by a pedestrian, so surveillance measures are preferred.

Electronic Security

ACCESS CONTROL DEVICES

Access control devices are utilized to control access through a portal.

Card Readers

Card readers are used in access control systems to read a credential that allows access through access control points, typically a locked door. An access control reader can be a magnetic stripe reader, a bar code reader, a proximity reader, or a smart card reader. For the purposes of this guidance document, this section will address proximity and smart card readers, as these are the most commonly used devices.

A proximity card reader contains an antenna that energizes a second antenna mounted in an access control card when the card is presented within 3–5 inches of the reader. When the card's antenna is energized, it automatically transmits the card's unique security code to the proximity reader. The security code is transmitted in a Wiegand format, defined as 26-bit or 35-bit. The 26-bit format is typical for proximity cards, while 35-bit is used for smart cards.

Smart cards, which operate similarly to proximity cards, also contain a memory chip that can be used to store biometric templates or payment applications. This embedded memory chip makes smart cards more secure than standard proximity cards.

Any of the above card reader technologies can be used in conjunction with a PIN to provide dual authentication for higher security controls.

Biometric Reader

Biometric readers utilize unique “information you have”—such as fingerprint, hand geometry, iris, facial details, or vein patterns—in order to control access through a secured portal. Biometric readers increase the level of security at access control doors by providing positive verification of the individual requesting access.

Biometric readers work by comparing an enrolled biometric template to the biometric template of the item (e.g., fingerprint, iris) being presented at the reader. Access is only granted if the templates match. The user's enrolled template may be stored on a smart card, locally at the biometric reader, on the ACS server, or in a combination of locations.

Access Control Panel

An access control panel provides distributed intelligence between the access control devices located at the controlled portal and the access control server. When an access control card is presented to the card or biometric reader, the unique security code/biometric template is compared against the cardholder database. If the user is authorized to access the secure portal, the access control panel will unlock the door, which will remain unlocked based on the time properties programmed in the access control panel. Conversely, if the code/template does not match, access will not be granted through the portal. All transactions are recorded locally at the access control panel and transmitted to the ACS server for record.

The configuration of the access control panel can be centralized or distributed. In the distributed application, the panel is dedicated to a door/portal and provides a level of local intelligence at the door. In the centralized application, the access control panel is in a secured location (e.g., IT closet) and designed to support multiple doors/portals simultaneously. In either configuration, the access control panel serves as the communication hub between the end devices and the access control server.

Power Supply

Power supplies are required for security systems to support access control panels, electronic locking devices, video surveillance cameras (if not PoE-enabled IP cameras), and selected active alarm detection/annunciation devices (e.g., motion detector, horn/strobe). The power supply is designed to convert 120VAC to 12/24VDC to power the respective device(s). Most power supplies include a battery backup option to provide backup power when primary power is lost, or bridging power when transitioning from normal to emergency power.

ELECTRONIC LOCKING DEVICES

Electronic locking devices are used to electronically lock doors that require card access control, or to remotely unlock the door. The type of electronic locking devices should be selected based on the security requirements, and should be installed per code requirements.

Electric Lockset

Electric locksets are direct replacements for standard door-mounted mechanical locksets. The primary difference is that electric locksets contain a powered solenoid and integrated signal switch. The solenoid energizes to either lock or unlock the door depending on the configuration of the electric lockset (fail safe versus fail secure). Electric locksets may be integrated into a standard door handle or a panic hardware/crash-bar system.

Electric Strike

An electric strike (also known as an electric latch release) is installed to replace a standard door strike plate on the door frame. Electric strikes secure a door by holding the door's latch in the strike plate. When the strike plate is energized, it releases the door latch so that the door can be pushed open. Electric strikes are typically not recommended for high security doors as this lock can be easily attacked and bypassed.

Magnetic Lock

A magnetic lock (informally called a mag lock) utilizes a powered magnet (mounted on the door frame) and corresponding metal plate (mounted on the door). When power is applied to the magnet, the magnet and metal plate bond and secure when the door is closed. As magnetic locks do not provide immediate egress, fire marshals and authorities having jurisdiction have established strict code requirements for the use of this type of lock. Therefore, code requirements should be reviewed carefully prior to implementation of this type of electronic locking device.

Shear Lock

A shear lock operates like a magnetic lock, but is mounted between the door and frame and is not visible. This type of lock enables a door to swing in either direction. The challenge with a shear lock is that the door needs to perfectly return to the zero-position (closed and aligned with the door frame) for the lock to properly engage. The lock will not engage if the door is not perfectly centered. Unbalanced air pressure from HVAC systems could result in the door being unable to perfectly align in the closed position—though this may be a minor maintenance issue.

INTRUSION DETECTION DEVICES

Intrusion detection devices are used to detect the status of a portal or defined area.

Door Position Switch

A door position switch is based on an electric switch, typically operated by a magnetic field between the switch and magnet. When the door is closed, the switch and magnet align and either close or open the circuit signaling the door status to the ACS.

There are two primary types of door position switches: reed switch and high security switch. The reed switch is the most common type but is also the easiest to defeat as the magnet and the switch are not paired. This means that any magnet can activate the switch. A high security switch’s magnet and switch are paired, so that only the paired magnet can trigger the switch, eliminating the possibility of a generic magnet activating the switch.

Motion Detection

There are multiple different types of motion detectors, which fall generally into two categories: active and passive. Active motion detectors utilize a transmitter and receiver to detect when an object crosses the detection zone. Passive motion detectors only detect a change in the environment. As a result, passive motion detectors are typically less effective in detecting motion. The type of motion detector selected needs to meet the functional requirements and the installation environment requirements.

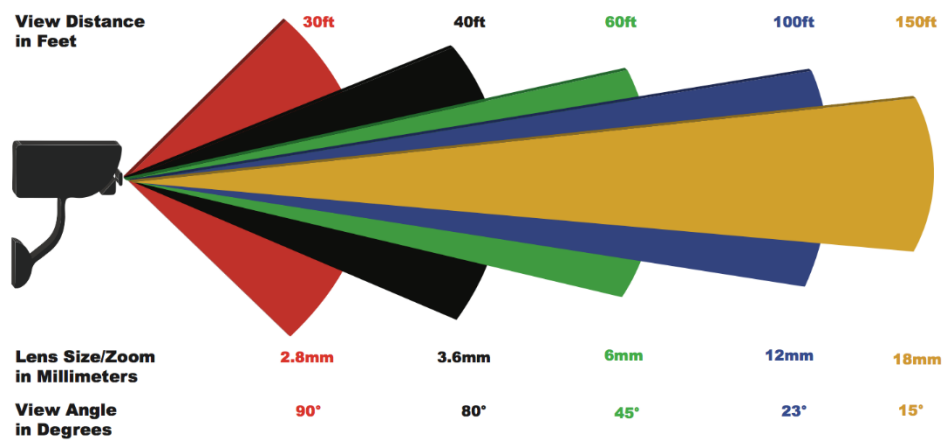
SURVEILLANCE CAMERAS

Surveillance cameras are grouped into five primary categories: standard fixed, pan/tilt/zoom, multi-imager, panoramic, and infrared (thermal) imagers.

Fixed Single-Imager Camera

Fixed single-imager camera (fixed camera) is the most common camera type. Fixed cameras consist of a single lens mounted in a housing (e.g., dome, bullet, box) with a fixed or varifocal lens. A fixed lens has a specific size, stated in millimeters (mm). A varifocal lens is provide a ranges of lens sizes. Varifocal lens provides an advantage in that once the camera is installed, the installer can fine-tune its field of view.

Figure 31. Single Fixed-Imager Camera



Source: Insyte Security

High megapixel fixed cameras (20MP and greater) are capable of viewing large areas and enabling digital

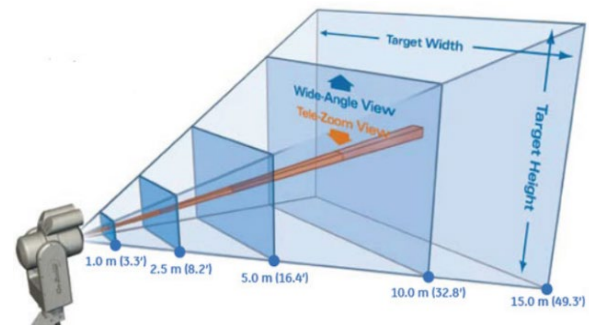
zooming on the fixed image. Although these cameras do provide extremely high pixel counts and therefore greater resolution, they are challenged by the frames per second that can be transmitted. Typical applications for these types of cameras are large open areas, such as parking areas.

Inherent to fixed cameras, multiple users can view the same camera simultaneously based on the number of outputs streams from the camera and the configuration of the network.

Pan-Tilt-Zoom (PTZ) Camera

A PTZ camera is a camera that has a zoom lens and is mounted on an integrated positioning motor. PTZ cameras have the ability to move and zoom into specific areas of interest, and then back to a home position view, which typically covers a larger area for general surveillance. It should be noted that when zooming in on an object with a PTZ camera, the field of view narrows and carries a corresponding loss of overall situational awareness. Figure 32 shows an example PTZ field of view under wide angle (blue) and tele-zoom (red) conditions; only one view is achievable at a time. As a result, PTZ cameras are typically deployed as secondary/support cameras.

Figure 32. PTZ Camera Field of View Example



Source: IPVM

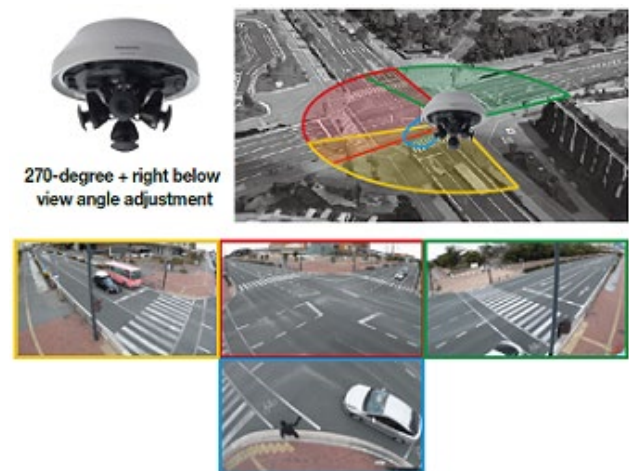
There are two key challenges to consider with PTZ. It is a common complaint that “PTZ cameras are never pointed in the direction of an event.” While anecdotal, there is truth to this statement. For this reason, it is not typically recommended to use a PTZ camera as a primary surveillance camera, especially in high security areas.

The second challenge with PTZ cameras is the “Ownership of Control” for the camera’s movement. As VMS platforms enable multiple authorized users to access cameras simultaneously, there is a potential for two users to attempt to control a single PTZ camera. This risk can be mitigated by providing priority levels to user access—typically security operators have the highest level of control and emergency management a lower level of control. But this type of mitigation assumes a static level of control need, and could be problematic in some scenarios, such as a breach of a SIDA door into the AOA with a simultaneous fuel spill at the same gate area. Security will need to utilize the PTZ camera to search for the individual who breached the door, while emergency management will also need access to the camera to assess the fuel spill situation. Because security has the higher level of control, emergency management would not have access to the PTZ camera, which therefore would potentially impact their ability to assess the fuel spill event remotely.

Fixed Multi-Imager Camera

Fixed multi-imager cameras consist of two to four fixed imagers mounted within a single dome enclosure. The cameras’ lenses can be fixed or varifocal. Multi-imager camera usage continues to grow as they are an attractive option for covering wide areas compared to multiple fixed cameras.

Figure 33. Multi-Imager Field of View Example



Instead of using a single lens with a super wide angle of view, typical in fisheye models, each of the imagers in a multi-imager camera has a narrow angle of view, which combine to cover a wide area. These applications can provide a 180-degree panoramic view, 270-degree view when mounted on a corner or down multiple corridors, or a 360-degree view.

Figure 33 provides an example of a multi-imager camera that has three lenses configured to view three directions and the fourth lens to look directly down to eliminate blind spots below the camera.

Multi-imager cameras do not require any dewarping. The video from each imager is “flat” like any traditional camera. The only difference is that when the video scenes are stitched together, the result has a far wider aspect ratio. Since this can cause problems in VMS layouts, often the non-stitched views are easier to display. In addition, since this camera solution provides individual view streams, it does not support any immersive (three dimensional) controls.

Because multi-imager cameras do not require dewarping, VMS integration is typically feasible, but licensing requirements vary by VMS manufacturer. Some VMS platforms only require a single license because it is viewed as one camera, or charge only a single license per IP/MAC address. Others charge a license for each imager, since the camera contains multiple imagers and produces multiple feeds.

Multi-imager cameras have two notable limitations. Advanced features such as high end, true wide dynamic range and super lowlight capabilities are not common in repositionable multi-imager models; integrated IR is unavailable. The second limitation is that multi-imager models often support a maximum of 15–20 fps or less on all channels, while single imager models are capable of 30 fps. However, the fps has been improving across manufacturers, getting closer to reaching 30 fps.

Fixed Panoramic Camera

Fixed panoramic cameras use a single super wide-angle lens or fish-eye lens positioned downward in a dome housing, providing viewing capability in every direction. However, the broader the area covered by the camera, the lower the pixel density/ppf it can provide, which significantly reduces the details in the camera view.

Fisheye images are typically not used in their normal, warped state (Figure 34), as the top-down view is less useful for monitoring, with some objects/subjects appearing upside down or sideways, depending on their location in the room. To make them more usable and flattened like typical surveillance video, they are dewarped by special software.

This dewarping is a critical component of panoramic cameras. The video image can be dewarped at the camera side, client side, or both. The choice of where to dewarp impacts VMS integration. Dewarping fisheye cameras typically requires a separate SDK for each manufacturer.

Panoramic cameras have historically been especially poor in low light, often displaying noisy or dark images in even slightly low light. Owners should beware when specifying fisheye models in even moderately low light (3–5 lux), as noise and artifacting/image ghosting is possible.

It should be noted that when the camera’s images are dewarped to provide multiple flat views, the images are considered edited. This editing could result in the inability to use the images for legal or prosecution purposes. As a result, these types of cameras should not be used as primary surveillance for regulatory doors.

Figure 34. Panoramic Field of View Sample



Source: FLIR

Infrared (Thermal) Cameras

All objects give off heat to some degree, and that heat is made up of long wavelength infrared radiation that the human eye cannot see. Thermal imaging sensors render this radiation as a visible light picture. Not only does this picture help us identify objects in total darkness, or through dense smoke, but the sensor information can be used to measure temperature differences as well.

Thermal camera technology provides the ability to detect extremely small differences in temperature with no light or special illuminators, and may not be limited by smoke, fog, or other particulates. The optics used with thermal imagers have the same fundamental characteristics as video cameras or lenses, with selections made by focal length and f-number (relative apertures).

Performance requirements should be established during the PDD. Emphasis should be on what level of surveillance is needed and how the imagery will be used—e.g., for area surveillance and to assist response teams, or for forensics—with due consideration for operational limitations. Glass penetration, for example, is possible only with short wavelength infrared sensors; mid-wavelength and long-wavelength sensors cannot see through most window glass.

Video and thermal imagery fusion is another issue to be addressed in the PDD. Imagery fusion is a process that is able to combine images from a thermal camera with images from video surveillance cameras and image-intensified night vision cameras. This can be especially important at night, when lighting is poor and supplementary lighting is not possible, and during conditions of poor weather where thermal cameras excel.

VIDEO SURVEILLANCE CAMERA STANDARDS

This section will address software standards applicable to camera systems.

ONVIF

ONVIF (Open Network Video Interface Forum) is a global and open industry forum that was formed to facilitate the development and use of a global open standard for physical IP-based security products. The forum aims to standardize how IP products within the video surveillance industry communicate with each other.

The organization was started in 2008 by Axis, Bosch, and Sony with open membership for manufacturers, software developers, consultants, system integrators, end-users and other groups that want to participate. The core concepts of the ONVIF standard are standardization of communication between IP devices, interoperability between network video products no matter who the manufacturer is, and that the standard is open to all companies and organizations.

ONVIF has several benefits for IP products. The open standard allows for interoperability of products from different manufacturers because they essentially speak the same language. This provides flexibility since end-users and security integrators are not locked into proprietary technology from individual manufacturers. Under the open standard, there will be interoperable products on the market no matter what happens to individual companies.

ONVIF has established a series of profiles within the standard. ONVIF profiles make it easy to recognize which ONVIF-conformant devices and clients are compatible. An ONVIF profile has a fixed set of features that must be supported by a conformant device and client. It ensures that a client that conforms to Profile S, for example, will work with a device that also conforms to Profile S. There are also conditional features, which are features that shall be implemented by an ONVIF device or ONVIF client if it supports that feature in any way, including any proprietary way. The

four profiles that are relevant to video surveillance systems are G, Q, S, and T. These are defined as follows:

- S is the oldest and most broadly supported profile, covering video streaming and the basics of sending video from a camera to a VMS/recorder. Most manufacturers support S.
- G supports accessing video storage. For example, retrieving and sending from an IP camera with onboard storage to a VMS/recorder.
- Q aims to simplify discovering cameras and improves security by eliminating default passwords. It was officially adopted as of July 2016, but has little manufacturer support.
- T improves integration of H.265, motion, analytics, and other events, as well as advanced settings such as exposure, focus, contrast, etc.

The key takeaway with ONVIF is that just because a device is ONVIF compliant does not mean that it will be universally managed by a VMS. It is still critical as part of the design to ensure the IP camera is supported by the VMS.

H.264

H.264 is a video compression standard that utilizes motion-based, block-oriented coding to create highly compressed, high quality video streams. This standard is also referred to as MPEG-4 Part 10 or Advanced Video Coding (MPEG-4 AVC). H.264 is currently the most widely used video compression format for the transmission, recording, and distribution of surveillance camera video streams.

H.264 compression was a significant improvement over earlier compression algorithms (MPEG-2, Motion JPEG [MJPEG], etc.) for the transmission of IP video over data networks. Unlike other compression algorithms, H.264 divides the video into an I- and P-frames. The I-frame (also referred to as a keyframe) contains all the pixel information. P-frames are the subsequent series of frames where only the parts of the scene that changed from previous frame are transmitted (as illustrated in Figure 35). During the transmission of the P-frame, the network bandwidth load significantly reduces, which makes this compression algorithm network friendly. When the I- and P-frames are received at the recorder/workstation, they are reconstructed to complete the image data. Although this encoding method reduces network traffic, it does significantly increase the processing power needs at the workstation to re-assemble the frames of video.

Figure 35. I-Frame vs. P-Frame



Source: Open Frame works

H.264 vs. MJPEG Quality

While H.264 is currently the most widely used codec in surveillance, for many years there have been debates about the loss of video quality compared to MJPEG. MJPEG transmits only I-frames, but compresses every I-frame. Although the network overhead and storage requirements are higher with MJPEG, there have been industry opinions that MJPEG is better for video recording. And since every frame is transmitted, there is no loss of background information. The same quality can be achieved with H.264 compression, but it does increase network and processing power to support

these larger files. In order to balance quality versus file size, the H.264 stream from the camera is typically utilized for live viewing while a second stream utilizing MJPEG compression is transmitted to the video storage system. The PDD should state the configuration of the recording video stream and confirm the level of quality and the compression method to be used.

H.265

H.265 has been discussed in the industry for the past few years as the next big codec, promising to replace H.264 and reduce bitrates by another ~50% under maximum compression settings. However, there are several key barriers preventing its widespread implementation:

- **Limited gains:** While the change from MJPEG to H.264 resulted in drastic bit rate reductions, often 50–75% or more, H.265 show that 15–30% savings over H.264 is more likely, while still maintaining the image quality compared to H.264. Given this fact and the rapid increase in size/decrease in cost of data storage, the benefits of H.265 are not as compelling as its predecessor.
- **Increased CPU load:** Viewing H.265 streams requires significantly more processor load than equivalent fps/resolution H.264 streams. In some cases, depending on the level of activity, double processing power could be required for viewing workstations. As processing power for workstations increases with GPU processing capabilities, H.265 becomes slightly more feasible.
- **Development required:** Current VMS platforms support H.264. Supporting H.265 camera compression may require significant costs to upgrade/replace the VMS.
- **Limited ONVIF conformance:** Moving to H.265 cameras has meant giving up true ONVIF conformance until the completion of their latest profile, Profile T, which was released in Q4 2018 with limited conformant products. Camera manufacturers were able to implement H.265 using ONVIF's 2.4 spec, but there was no conformance test until this profile was complete. Profile T cameras increased rapidly in 2019/2020, but VMS conformance is still limited to a handful of recorders.

Proprietary

The video surveillance industry still has had a limited number of proprietary codecs in use at the time of this document development. Although these solutions can provide better storage management and network data traffic, these types of systems are required to be proprietary from camera to recorder. This level of end to end proprietary control will typically result in higher equipment costs and even greater costs if the camera or VMS needs to be replaced. Proprietary compression should be avoided unless specifically requested by the owner. Axis Zipstream is a notable exception to this statement. Although the Axis Zipstream is a proprietary compression method, many VMS manufacturers have developed an interface to support it.

Smart Compression

Although not a specific compression method, most camera systems employ the use of a “smart compression” algorithm to further support improved network bandwidth utilization and storage. For example, if implemented for a camera mounted in a hallway, the background walls would be set to high compression, since this surface does not change and has limited details; activity in the scene would be set to low compression to ensure a higher quality image is captured.

Another type of smart compression is in relation to the detection of motion. Taking the same example of a camera in a hallway, when there is activity in the camera's field of view, it will record

and transmit video at the defined functional requirement. When there is no activity detected in the field of view, the record and transmit settings (typically both fps and resolution) will reduce.

VIDEO MANAGEMENT SYSTEMS (VMS)

A VMS is composed of software and hardware. The software is custom to the VMS application and provides the control, management, storage, and system intelligence to manage the cameras connected to the VMS (analog with video encoders and/or IP). The VMS manages the database of cameras including device naming, recording profiles, playback controls, and user log-in with permissions. The VMS application provides the interface for users to control, view, manage, and export video images.

The hardware consists of the management and storage servers. Depending on the manufacturer, the management server and storage server may be the same device. The management server stores the database of the users and permissions, the cameras, and interfaces to third-party systems (e.g., ACS for alarm call-up functions). The storage server is where the recorded video is stored based on the recording profile identified in the management server.

Both the management server and the storage server can be configured for redundancy. The level and type of redundancy should be coordinated based on the requirements of the PDD.

PERIMETER INTRUSION DETECTION SYSTEMS (PIDS)

PIDS are utilized to detect an unauthorized person or object penetrating into the AOA. There are a variety of technologies that may be considered, each with advantages and challenges to the deployment solutions. The type of system selected should be based on the installation conditions, probability of detection requirements, and lowest false alarm rate.

Radar Systems

Radar systems are designed to provide volumetric, all-weather (in most cases) surveillance. Radar systems are able to search a wide area, detect and track an object, and provide accurate object location information, usually within seconds.

Generally, there are two primary types of radar systems for use as intrusion detection systems. These are defined by the method each employs to detect objects: (1) detection based on the frequency shift of a returned radio signal caused by the movement of an object, known as Doppler radar; and (2) detection based on the amplitude or strength of the returned radio signal, referred to here as a non-Doppler radar.

A radar system's range and azimuth resolution are dependent on system characteristics such as operating frequency, pulse width, radiated power, and antenna beam width. In general, the most commonly found commercial perimeter intrusion detection surveillance radar frequency is X-Band (~10GHz) system, with higher-band radars (35GHz and up) reserved for the specialized functions of high resolution, short-range detection. However, other frequency-band radars, such as Ku-Band (16GHz) radars, C-Band (5GHz) and S-Band (3GHz, marine radars) are also used for perimeter intrusion detection.

The radar system's resolution determines the radar's ability to distinguish between closely spaced targets.

Radar sensors provide target location information to an auxiliary processor to determine if a perimeter has been breached. This auxiliary processor should use the radar detection/track information to calculate the target location relative to a protected asset (e.g., a shoreline keep-out zone, a protected building, or a fence line) to establish whether an alarm should be generated.

The type of radar should be selected based on the deployment locations and detection needs. Radar systems are typically integrated with assessment cameras to view and assess alarm events.

Lidar Systems

Lidar (Light Detection and Ranging) systems employ light waves, in a manner similar to how a radar sensor employs radio waves, to provide target distance and bearing information, and discriminate among targets based on size.

Lidar systems must have a clear line of sight to detect a target. Obstructions, direct sunlight (cannot point upward to sun), and sensitivity to object color (e.g., shiny black objects) are problems that must sometimes be adjusted for. Lidars can be mounted high on buildings to provide better line of sight. Forested or densely urban areas are not well suited for lidar surveillance.

Extreme weather conditions will reduce the usable range. Particles in the air, such as smoke, smog, and fog can also interfere with the sensor.

Lidar systems can discriminate blowing debris from actual intruders. They are not affected by EMI.

Lidar systems must satisfy eye safety standards and be approved for airfield use by the FAA.

Lidar systems do not perform target assessment and should be augmented with assessment cameras.

As with radar, lidar systems should be tested in the airport environment using targets moving at varying speeds (e.g., humans stationary, crawling, slow walking, walking, jogging, and running) through the different types of terrain the system will be deployed (e.g., smooth pavement, grassy fields, hilly areas, water areas, brush, or tall grassy areas). Vehicles and watercraft targets should also be tested as appropriate to the proposed deployment area.

Infrared Beams

A frequency-modulated, multiple beam pattern of infrared energy exhibits changes in the modulation frequency or interruption of that beam when a target crosses it. This function can be used for intrusion detection. Infrared beams have a typical range of up to 1,000 feet and can detect objects walking, running, jumping, crawling, rolling.

Infrared beams are subject to false alarms due to fog, heavy rain, smoke, and wind-blown particulates. This system can be susceptible to tunneling, trenching, bridging, and climbing as the detection zone is clearly identified by the transmit and receive towers. If deep enough, snow may block the lower beams, giving no detection if someone crawls across in the snow. This solution is best applied in flat terrain.

Passive Infrared Area Sensors

Passive infrared areas sensors detect changes in thermal radiation (i.e., temperature and target emissivity) due to objects passing through the sensor's field of coverage. The detection range is typically limited to 50 feet and can detect objects walking and running objects.

Passive infrared sensors have difficulty detecting targets at or near the ambient temperature of the environment. Objects moving toward the sensor will have a lower probability of detection compared to the object moving across the detection field.

Fence Vibration Sensors

Fence-mounted PIDS typically operated by sensing fence vibrations associated with intrusion activities such as cutting or climbing. The range of these system depends on the manufacturer solution, but the typical detection zone along a fence is 10 feet.

Fence vibration sensors require a mechanically sound, stable, and well-maintained fence. This type of system is susceptible to false alarms caused by anything that might shake or vibrate the fence. In an airport environment, these may include wind, rain, windblown debris, large birds, etc.

Fiber Optic Cable

Single or multiple fibers can be mounted to a fence, walls, or underground to detect climbing, cutting, and intrusion. Optical signals transmitted simultaneously clockwise and counterclockwise over the same optical cable will exhibit interference at or near the point of an intrusion; the event can be detected using several techniques including interferometry and specular pattern changes. The range of these systems depends on the manufacturer solution, but is typically several kilometers.

Fiber optic cable sensors provide a higher level of sensitivity compared to other cable-based solutions. Since this type of cable is not impacted by electromagnetic interference (EMI), it is often utilized at utility plant or power stations.

Fiber optic cable sensors require a mechanically sound, stable, and well-maintained fence. Windblown debris can result in false alarms.

Buried Line Sensor

Buried fluid-filled cable in plastic tubing can be used for intrusion detection. Typically, two tubes are buried approximately four feet apart along the length of the detection zone. The tubes are very sensitive to pressure changes due to targets moving across the ground. The typical detection range is up to 1,000 feet.

Buried line sensors are subject to high false alarm rates due to standing snow or water, water runoff, tree roots, animals, seismic energy, and may fail to detect objects moving slowly in the detection zone.

Ported Coax Buried Cable

Coaxial cables can be trenched into the soil at a shallow depth or slotted into asphalt or concrete tarmac to create an invisible perimeter. A small amount of electromagnetic energy is emitted by one coaxial cable and received by the adjacent parallel one to create a field of energy where disturbances can be sensed. The sensor cables also carry their own power and communications data, so no other infrastructure is required.

Continuous wave ported coax sensors are deployed in multiple blocks, up to 500 feet each, and provide intruder location to the individual block. Pulse or broadband sensors use cables up to 1,300 feet each and indicate intrusion location to within a few meters, so they can be used for precise aiming of cameras to detection areas of the perimeter. With the newer broadband systems, segments of the sensor cable can be electronically configured into multiple zones to be accessed from the central control station.

Ported coax buried cable must be run free of non-sensor electrical power and control cabling, and the surface area must be clear and unencumbered. Bridging of the detection field is possible, but difficult with proper cable spacing and covert burial. Windblown debris, standing water or metallic debris over the sensor cables, large (human-sized) animals, lightning, and EMI are potential nuisance alarm sources. In frost-prone areas, seasonal recalibration for sensitivity increases in frozen ground

is recommended. Though the sensor is not vibration sensitive, prescribed separation from vehicles on nearby roadways, or trains is required to avoid nuisance alarms. Zone coverage with cables buried is covert and not visually apparent.

Bi-Static Microwave Beams

Microwave beams are suitable for flat areas that have an unobstructed line of sight. The transmitter and receiver are separate units. The detection field is invisible and fills the space between the transmitter and receiver. Stacking of units with different frequencies of operation or polarization, to prevent interference, can enhance detection capabilities.

Proper design requires overlapping coverage, i.e., each transmitter is within the beam coverage of another transmitter to avoid dead zones and the possibility of crawlers at the units not being detected. Bi-static microwave beams cannot be installed at locations with standing water. This system is prone to false alarms if there are large metal objects nearby, or in windy conditions.

Network Communication Systems

NETWORK DESIGN OBJECTIVES

It is critical to set clear objectives at the outset of the network design process by identifying network performance parameters and setting target values, which will ultimately be dictated by the application requirements. To assign appropriate targets, the requirement should be expressed at both a quantitative and a qualitative level, e.g., stating the necessary transmission bandwidth, its sensitivity to packet loss, packet delay and variation in delay, etc. All of these are especially important on IP networks that support multiple heterogeneous applications, including voice and video.

Data applications that employ the User Datagram Protocol (UDP) for transport are more seriously affected by packet loss than connection-oriented TCP-based applications. UDP is a connectionless communication transport method. Unlike TCP, UDP does not acknowledge or guarantee delivery, nor does it provide sequencing of packets. Conversely, real-time applications such as voice, video, and multimedia tolerate packet loss better than they do delay and variations in delay (jitter).

Target values should also be set for network availability or downtime in unambiguous terms, including how such targets are to be validated and tested. In a shared IT environment, where security is one of several applications on the network, IT policies for availability and downtime should be revised against security requirements, including zero downtime for critical functions.

NETWORK TOPOLOGIES AND ARCHITECTURES

The common Ethernet architecture calls for three network tiers: the network core, the distribution (or aggregation) layer, and the application (or access) layer with Gigabit Ethernet (GbE) equipment at network cores, 1 Gigabit (Gb) equipment in the distribution network, and 1 Gb or 100 Megabit equipment for applications. Local area network (LAN) attached devices are connected to access switches, and aggregation switches are then connected to core routers/switches that provide routing, connectivity to wide-area network (WAN) services, segmentation, and congestion management.

With the availability of 10 Gb and higher bandwidth core equipment, it may be possible to flatten the network by eliminating the distribution (aggregation) layer. The IEEE-803ba Standards working group has approved a 40/100 Gb/sec Ethernet.

The latency inherent in a three-tier approach should be examined when video is a major network payload. For video transmission, a network using 10 GbE or higher data rate equipment can reduce end-to-end streaming delays (latency), resulting in improved video transmission across the network. Also,

because it provides an opportunity to use a two-tier network architecture that will result in fewer switches to install, operate, and manage, it may also reduce equipment acquisition and maintenance costs.

NETWORK BANDWIDTH

While consumed or delivered bandwidth may be much less than the interface bandwidth, Ethernet connections—especially client-facing connections—operate at a fraction of the available bandwidth, thanks to the bursting nature of the data traffic. Except for WAN connectivity of large data centers, historical evidence for service provider leased lines and data services also points to LAN and WAN connection utilization far less than 100 percent.

Oversubscription is inherent in the design of hierarchical networks. This is a common means of maximizing the number of customers served while minimizing the hardware cost, which is a practice carried over from telecommunication networks that typically provisioned one telephone circuit for each 10 telephone subscribers. Oversubscription lowers costs by sharing common components, such as network processor units, and optimizes their utilization. The user interface currently ranges from 10/100 Ethernet to 1 Gb and 10 GbE. To minimize the degradation of network performance in cases of congestion, and to ensure that critical traffic is transmitted, intelligent oversubscription should be implemented.

Oversubscription by itself, however, is insufficient. When full system-side bandwidth is consumed, the tail-drop method of traffic queue management is implemented where select data packets are dropped and queued until there is sufficient capacity. If the last traffic into the system is voice, it is positioned behind email and web traffic; the voice traffic will be dropped and/or voice quality will degrade significantly.

The network designer will need to address means to offer the same type of capabilities—quality of service (QoS), bandwidth guarantees, and traffic shaping—regardless of port speed or whether the port faces the customer or the network.

When an airport VSS is networked, special design consideration must be given to such issues as transmission bandwidth over the network, network headroom allowances, and video storage, including image resolution and frame rate, storage duration, and permissions for accessing and viewing stored images. This portion of network architecture may involve both centralized and edge-based assets. Video streaming is a major consumer of bandwidth and needs to be carefully considered in the design and configuration of the network.

QUALITY OF SERVICE (QoS)

QoS addresses the ability of a network to guarantee different levels of service to selected traffic. The goal is to prioritize certain traffic flows without making other flows fail, thereby ensuring consistent, guaranteed performance for the selected priority traffic. QoS provisioning is essential for a network carrying video traffic, as well as data traffic, because it protects critical streams against packet losses and delays by monitoring and prioritizing traffic, and by managing LAN and Wireless LAN (WLAN) bandwidth.

General data traffic is often tolerant of delays, e.g., most users are not sensitive to brief email delays. However, video traffic is time-critical streams and has different requirements for quality performance. By adding QoS, critical applications such as video systems receive priority queuing, so the traffic is shaped according to the stream profile before being transmitted over the network. QoS should be a major design consideration to ensure that important traffic gets the required level of service.

BANDWIDTH MANAGEMENT

Usage of digital technologies for VSS has increased the typical airport network bandwidth requirements. However, communications network technologies have improved data transmission rates enough to enable airports to design 10 GbE networks. The requirements for frames per second, frame size (video resolution), and video compression methods will ultimately determine the bandwidth requirements of the VSS network.

During the design phase, it is important for the airport communications network to be sized for worst case scenarios—present as well as future—in terms of bandwidth. In this hypothetical situation, multiple airport security and operations personnel would need maximum and possibly simultaneous use of the networked equipment for activities such as examining live and recorded video from multiple cameras. This could easily require 10 to 20 times the normal network capacity needed for security. Unlike business applications that have easily established activity patterns in terms of network load, security systems, especially VSS, can be moderate until an alarm or security incident occurs, introducing immediate heavy demands on top of continuing normal loads.

ACTIVE INFRASTRUCTURE

Many airports are establishing shared communications infrastructures to support all low voltage operational systems throughout their campuses. These systems include, but are not limited to administrative networks, voice systems, Electronic Visual Information Display Systems, Common Use Passenger Processing Systems, public address systems, building management systems, VSS, and ACS. Using this approach, airports can achieve economies of scale by implementing communications infrastructures that provide fault tolerance and resiliency at much lower overall costs than if the individual components were implemented as standalone systems. When considering deploying and operating security systems over a common network infrastructure, the security systems should utilize dedicated Virtual LANs to create a logically separate network for the security systems. This will ensure that security network traffic is appropriately prioritized and afforded the speeds required to support security data traffic, especially video streams.

PASSIVE INFRASTRUCTURE

Passive infrastructure is the physical cabling (copper cabling or fiber optic cabling), routing infrastructure (i.e., conduit and cable tray), patch panels, splicing equipment, and termination hardware used for the interconnectivity of communications systems throughout the airport.

Planning and design of the cabling infrastructure for security systems can play an important role in efficient installation and aesthetics, and, more importantly, in system security and maintainability. A well-designed passive infrastructure system can reduce repair times and costs; minimize system and equipment downtimes; and reduce the cost and time required to expand, modify, or upgrade systems. As security systems are critical to airport operations, reduced multi-year repair times alone warrant careful consideration of these issues.

If security and common-use data cabling are of the same quality and offer spare capacity, each may provide an alternate route for mission-critical applications of the other (i.e., redundant cable paths). Physical separation of the security and data network cables reduces the risk of compromising security; however, in the event of cable damage in either network in an integrated system, a simple cross connect can restore services more quickly, if only on a temporary basis while more complete repairs are performed.

Measures should also be taken to protect cable security. Cables, connections, and equipment should be protected from accidental damage, sabotage, and physical wiretapping. This is usually accomplished by placing security-related cabling in secure areas. When cabling must pass through public areas, it should

be protected by metal conduit or electrical-mechanical tubing, and this should extend to telecommunications rooms where the security-related cabling terminates.

When selecting the type of cabling, there are limitations that need to be considered. Copper data cabling has a distance limitation of 295 feet (100 m) between the data outlet and IT closet. The result is that an IT closet or local equipment cabinet to support a network switch must be located within this distance to ensure the copper data cable can be tested as compliant. Fiber optic cabling has an average distance limitation of 3,000 feet (1,000 m), reducing the number of IT closets needed due to distance limitations. However, fiber optic cabling does have challenges in installation methods, and still requires a power source to each IP device. The type of cabling should be reviewed with the IT/Communications designer to determine the specific installation type and how it is able to support the security systems.

APPENDIX H: FUTURE AIRPORT CONSIDERATIONS

HIGH SPEED LANDSIDE SCREENING / SCANNING AT DISTANCE

One of the largest threats to an airport is the landside area. Individuals within this space are unscreened and have access to areas where large groups of individuals are queued. With the ease of access to high power weapons, active shooter events nationally will continue to increase and be one of the largest threats to airport landside areas.

High speed screening systems provide airports with the ability to screen individuals for weapons, specifically long barrel semi/automatic weapons. As these systems are high speed, they would not impact the flow of people entering the facility, but would alert security personnel to a suspect individual before shots are fired within the terminal. These systems do require additional security staffing at the screening stations, which could be challenging from an operational cost perspective. As these systems develop further, and terminals are redeveloped with security at the forefront, integration of these high speed screening systems into controlled entry portals could significantly reduce the security staffing needs.

SECURITY MANAGEMENT SYSTEMS (SeMS)

When developing electronic security systems, it is important to establish a robust security culture identifying a change management program to engage the entire airport community and to implement the necessary support mechanisms e.g. training and reporting systems. SeMS is a mechanism, or management technique, to establish and maintain a security culture, and to integrate security into the airport's business. SeMS is not a new security concept, but it has been slow to be adopted in the United States. Manage security risks while instilling security into the airport's business provides for more effective, efficient, and sustainable security. The culture aspect is consistent with the Safety Management System experience, which has proven that a positive safety culture results in improved safety through the reduction of safety hazards.

The establishment and maintenance of an airport-wide security culture, and the integration of security into the airport's business, is achieved by establishing and maturing seven elements that, when integrated with each other and the broader airport business, form an SeMS. The individual elements are critical components that work as a system to provide for collectively improved security outcomes. While this a long-term organizational culture change program, most measure are able to be implemented quickly and easily with outcomes that are sustainable. A robust security culture contributes to deterrence, detection, and overall risk reduction throughout the airport.

For additional information on this topic, refer to [PARAS 0009 – Guidance for Security Management Systems](#).³⁴

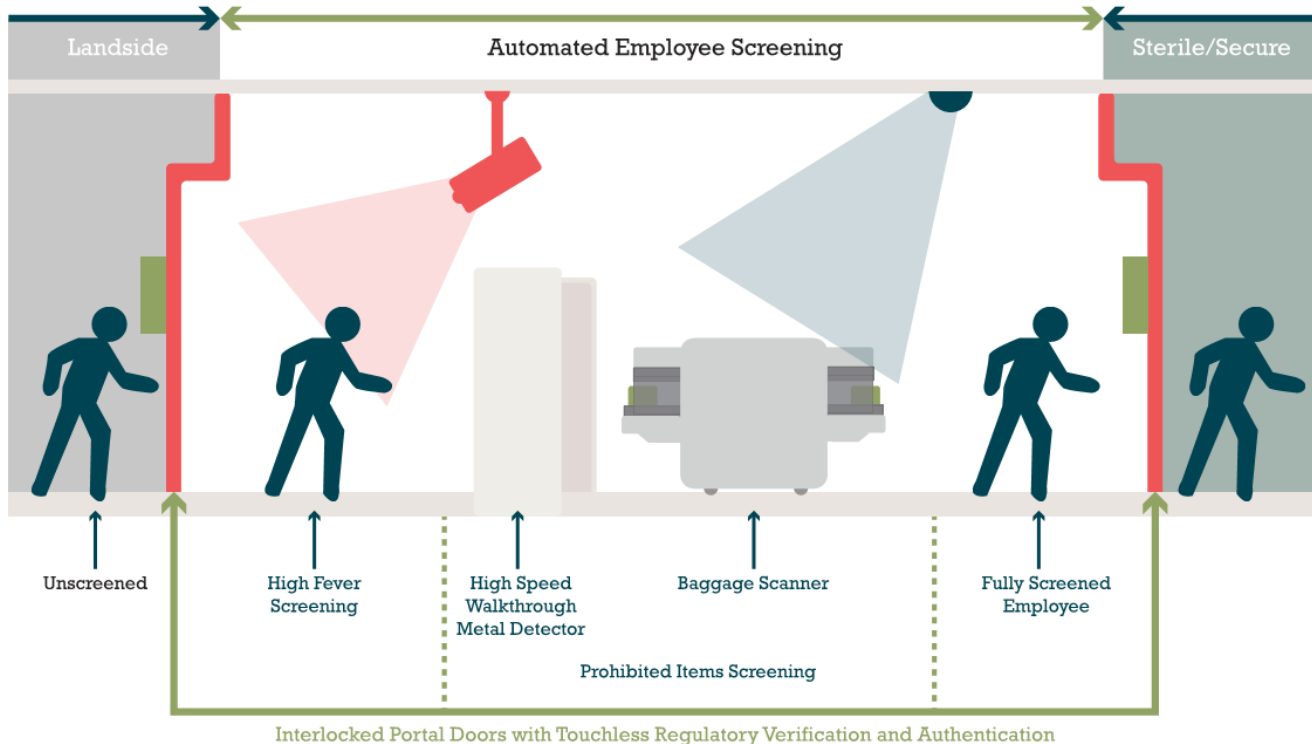
AUTOMATED FULL EMPLOYEE SCREENING

Airports are challenged with the goal to obtain full employee screening without adding load to the TSA SSCP. In response, airports have identified locations for dedicated employee screening, which typically relies on a manual process. A dedicated employee screening area should be considered for future new terminals or redevelopment projects. Figure 36 illustrates a proposed concept for an automated employee screening system. An unscreened employee approaches the screening portal and presents their credential for verification. In the example and post-COVID-19, the verification system would be a touchless biometric technology (e.g., iris scanner, face scanner, or palm vein scanner). If there are no employees undergoing the screening process, the landside door would open. The employee would then

³⁴ For download: https://www.sskies.org/images/uploads/subpage/PARAS_0009SeMS_Guidance-Final.pdf

be temperature screened to assess for health concerns, before entering the walkthrough metal detector and then placing any objects onto the baggage scanner. Similar to the remote-screening concept utilized at the SSCP, a remote operator would verify that the employee does not have any prohibited items among their belongings. If cleared, the employee would again present their touchless credential to be provided access to the Sterile/Secured area. If a questionable item is detected, the employee would be directed to an adjacent holding room for additional screening.

Figure 36. Future Employee Screening Portal



OCCUPANCY DENSITY AND ANALYTICS FOR SECURITY ISSUE DETECTION

Airports continually gather data that is primarily used to track passenger movements and activity throughout the airport for marking purposes, cleaning needs, etc. This information is also extremely valuable for security purposes, to identify hotspot areas within the airport and any anomalies. When hotspots are identified, the security group can review the areas and, if needed, direct supplemental security to that area, such as video surveillance or additional security officers.

ONE-STOP SECURITY³⁵

One-Stop Security (OSS) is a European Union (EU) regulatory framework that provides for the recognition of the security procedures applied in a non-EU country, if those procedures are equivalent to EU standards. Recognition enables passengers, baggage, and cargo to forego security controls again when transferring at EU airports. The OSS concept is illustrated in Figure 37.

³⁵ For download: <https://store.aci.aero/form/one-stop-security-toolkit/>

Figure 37. OSS Concept



Source: ACI World

The goal of OSS is to more efficiently process passengers and baggage from airport to airport. OSS aims to expedite the flow of transfer passengers and baggage to their destinations by eliminating the unnecessary duplication of security controls at the transfer airport. The concept has been a topic for discussion for many years but is slowly making some inroads in the EU.

Although the OSS concept is currently focused on the EU, an ideal long-term perspective held by many in the aviation industry is for a global approach to the OSS process.

APPENDIX I: AREA-SPECIFIC SUMMARY DESIGN CONSIDERATIONS

General Airport Layout

LANDSIDE

As landside facilities do not directly affect the operation of aircraft, they generally have less stringent security requirements than the airside. Since these areas are publicly accessible, they still do have a high threat profile for landside attacks and PB/VBIEDs. They may also be used for public protests, which can require heightened security in the terminal area.

TERMINAL

When considering passenger and baggage screening security provisions, it is important to distinguish the commercial terminal from the GA terminal, where charter and private passenger activities typically occur. It is also important to note that security requirements may affect charter and private aviation as well as scheduled commercial aviation.

The terminal is often the area of the airport with the most security, safety, and operational requirements. Many of these requirements are closely linked to the locations of security areas within and near the terminal. Since the terminal usually straddles the boundary between airside and landside, certain portions of a terminal, such as baggage induction points at ticket counters, must meet the requirements of both areas.

When designing a new facility, the terminal is typically located centrally on the airport site. This not only provides for efficient aircraft access to most runways and facilities, but can benefit terminal security as well. A centralized terminal buffers the terminal from outside threats and security risks due to distance. A fundamental concept in security planning, distance provides the flexibility for the airport operator to put in place systems, measures, or procedures to detect, delay, and respond to unauthorized penetration. Providing additional standoff distance from a potential VBIED is highly beneficial when addressing blast-protection measures. A centralized terminal can also minimize the communications interference that might be caused by adjacent, non-airport facilities.

Security-Related Areas

Each airport's ASP, developed under 49 CFR § 1542.101, contains descriptions of the following areas in which security measures are specified at each airport.

AOA

The airport operator is required to control and prevent access to the AOA, control movement within the AOA, and control unauthorized penetrations of the AOA. TSA regulations do not specify how to accomplish this requirement, but leave the solution to the local authorities in a manner appropriate to their operating environment, subject to TSA approval.

In most cases, it is advantageous to align the AOA boundary with other boundaries or with physical barriers. The AOA is a major portion of the area within the fence or other barrier that defines the airside/landside boundary of the airport. Exceptions to this may occur when electronic barriers or natural barriers, such as rivers and coastal waterfront, are being used to delineate boundaries. However, when considering whether any natural barrier is an appropriate boundary, the airport operator should consider the findings of the airport TVA, and whether the natural barrier should be complemented with other types of boundary protection. Special attention should be given to areas near the airport boundary where

large bodies of water are used as public recreational or fishing areas. The AOA is required to have a distinct, securable boundary line.

SECURED AREA

Each Secured Area must independently meet all the requirements placed upon it by the ASP, including control of access, challenge procedures, LEO response, display of ID, etc., particularly where the various Secured Areas may not enjoy common boundaries or access points.

Where there are several unconnected Secured Areas, such as baggage makeup areas, movement areas, safety areas, etc., each may require separate but integrated electronic controls. Therefore, it is desirable to locate Secured Areas as close together as possible to maximize ease of access by response personnel, utilize common areas of video surveillance coverage, and minimize requirements for redundant boundaries and electronic access controls.

SIDA

Ordinarily, SIDA layouts should be held to the smallest manageable size to provide the level of protection sought for the area or facility. The SIDA is the area that requires the greatest continuous procedural attention from employees. The number of SIDA access points should be limited to the minimum necessary for operational practicality.

STERILE AREA

General security considerations of the Sterile Area include:

- All portals that serve as potential access points to Sterile Areas (i.e., doors, windows, passageways, etc.) must be secured to prevent bypassing the SSCP. The number of access points should be limited to the minimum that is operationally necessary, as determined by the airport operator.
- Portals, including gates and fire egress doors, must prevent unauthorized entry by any person to the Sterile Area, and to the Secured Area, which includes airside and baggage make-up areas. Guards are generally an expensive alternative to technology in this application. Doors must also comply with applicable local fire and life safety codes and ADA requirements, among others. Discussions with local building and/or life safety code officials should take place early to resolve special design issues, including how to secure fire doors, possibly with delayed egress hardware.
- Sterile Areas should be designed and constructed to prevent articles from being passed from non-Sterile Areas into Sterile or Secured Areas such as restrooms, airline lounges, and kitchen facilities, through plumbing chases, air vents, drains, trash chutes, utility tunnels, and other channels.
- When planning the construction of non-Sterile or public access suspended walkways or balconies over or adjacent to Sterile Areas, it is particularly important to consider effective barriers to prevent passing or throwing items into the Sterile Areas.
- During planning and layout of Sterile Areas, consideration should be given to the access needs of airport and airline personnel, and maintenance and concessions staff and supplies. Specific items for consideration include:
 - Tenant personnel and airport employees who require frequent daily access into the Sterile Area from public occupancy areas
 - Emergency response routes and pathways should be non-public, easily accessible, never blocked by storage boxes, bins, or other hazards, and provide clear, quick access for any emergency equipment needed (e.g., stretchers, wheelchairs, explosive detection devices,

transportation equipment, or paramedic equipment). Routes and access controls to accommodate off-airport response (e.g., emergency medical services and fire personnel) should also be considered, as well as the ID badging and access permissions necessary.

- Concessionaire deliveries and supplies should be considered as a part of the planning and design process. Concessionaires are often located within the Sterile Areas. Concessionaires and other airport tenants may receive deliveries at all times of the day, often from companies whose delivery personnel change frequently and cannot reliably be given keyed or media-controlled access into the Sterile Areas. Where possible, deliveries of this type should be limited to a non-Sterile Area and screened using appropriate hand searches, or explosives or x-ray detection methods, either through the SSCP or a dedicated screening process. Where loading docks are employed, they should not be adjacent to critical infrastructure such as HVAC, IT/communication centers, or emergency power generators, etc. The planning process should develop strategies for concessionaire deliveries, storage areas, employee access routes, and free flow. These require adequate attention to security levels to prevent obstructions and patron queuing near or in security checkpoint areas, and to eliminate the occurrence of unscreened delivery and concessions personnel within the Sterile Area. All such screening should take place well away from designated passenger screening areas.
- During construction or modification of facilities, provisions should be made to ensure that any individual who has not undergone screening is prevented from having physical contact with a screened person inside the Sterile Area.
- Security of Sterile Areas is improved with design solutions that deter the concealment of deadly or dangerous devices. Built-in fixtures (e.g., railings, pillars, benches, ashtrays, trash cans, etc.) designed to deter and/or hinder the concealment of weapons or dangerous devices are widely available.

EXCLUSIVE USE AREA

Specific requirements and conditions must appear in the exclusive area agreement, which is then approved by TSA. Such conditions include a very specific delineation of the areas for which the aircraft operator assumes security responsibilities. This does not include law enforcement responsibilities, which always remain with the airport operator. Like SIDAs and Sterile Areas, exclusive use areas should be held to an operational minimum so that appropriate surveillance and control resources can be concentrated where necessary, rather than scattered among less security-related areas.

PARAS 0025 *Security Regulatory Compliance at Tenant Facilities*, anticipated to be published in mid-2021, will cover this topic in more detail.

AIRPORT TENANT SECURITY PROGRAM AREA (ATSP)

Subject to a tenant area-specific security program approved by the TSA, the airport tenant assumes responsibility for specific security systems, measures, or procedures, but not law enforcement.

Where tenants other than air carriers elect to undertake under their own security programs under 49 CFR § 1542.113, such areas should be limited to the tenants' immediate boundaries and sphere of influence, and should accommodate security requirements for contiguous boundaries with other tenants and/or the airport and airlines.

Public Operational Spaces

PUBLIC AREAS

It is sometimes challenging to make the best possible operational, economic, and business use of terminal space, as well as to provide the passenger and public an acceptable level of comfort. The level of service concept in passenger terminals is generally discussed in terms of space requirements—whether the passengers will fit in an area or flow through it easily, and whether they will be comfortable doing so, particularly where they are occupying additional space with roll-on luggage. Security requirements are not always compatible with convenience and comfort.

Security is improved by reducing congestion and long queues at the curb and in public lobby areas. Large concentrations of passengers in public areas not only reduce the level of passenger service by limiting free movement but can become a threat target. Promoting the free flow of passengers requires adequate capacity at each successive stage, including curbside check-in, ticket counters, screening checkpoints, and vertical transportation, which should be calibrated to meet peak-hour flows. It is necessary to calibrate the capacities of spaces between the various processing elements. For example, the check-in time at the ticket counters should be calibrated to the time passengers spend going through passenger screening to avoid excessive queuing at either location.

DOMESTIC BAGGAGE CLAIM AREAS

Many of the baggage claim areas for domestic flights include vulnerabilities that can be addressed in new designs. Such features as accessibility from the street, bags stored on the floor in open areas, and conveyor belts that loop back through curtains into the SIDA should be eliminated or subjected to heightened surveillance and monitoring.

In contrast, claim areas for baggage arriving on international (non-preclearance) flights are not accessible from the street, and are completely within the airport's FIS Secured Area where no unscreened persons or bags enter. International baggage claim is much less susceptible to unwanted contact or access.

Airports may want to consider designing their domestic passenger routing and baggage claim areas to be within a secure area with no public access, similar to international arrivals. It is recognized that it is not practical to reconstruct domestic baggage claim areas in most existing terminals as stand-alone projects. However, when new terminals are being designed, or existing terminals are being extensively rebuilt and reconfigured, some aspects of the secure layout of international baggage claim areas may be adapted for domestic arrivals.

Some terminals have designed their arrival passenger flows so that both domestic and international arrivals are channeled directly via secure routings toward their respective baggage claim areas, so that there are no exit lanes adjacent to the screening checkpoint, thus mitigating a common security concern of checkpoint breaches.

PUBLIC EMERGENCY EXITS

Evacuation and exit requirements for public assembly buildings such as airport terminals are specifically established in building codes, including required widths and separation distances. However, exits required by building code may compromise optimal security planning. Without appropriate planning and design, emergency exit requirements can yield doors that provide inadequately secured access to restricted areas.

Consider equipping emergency exit doors with local and/or monitored alarms that can be responded to quickly by staff. The need and location of such emergency exits should be coordinated closely with the local fire marshal and code compliance officials. Whenever possible, the terminal building should be designed such that emergency exits leading into Secured Areas are minimized and exit ways avoid moving persons from a lower to a higher level of security area (i.e., from non-Sterile to Sterile, or from Sterile to SIDA or AOA). Likewise, screened individuals exiting under emergency conditions should be kept separate from unscreened individuals where possible. This may minimize the need to fully rescreen all persons in the case of an emergency or false alarm. Designers should also prevent travel in the reverse direction through emergency exit routes, to forestall undetected entry to Secured Areas during an emergency.

Particular attention should be paid to the potential for problems caused by mass evacuation, whether during an emergency or when a concourse has to be cleared after a breach. In either case, the designer should seek out optimal paths of travel, bearing in mind that those persons cleared from the terminal will require an area to be held, and possibly require rescreening prior to re-entry.

Where building codes permit, consider emergency exit doors with push-type panic bars that have 15–30 second delays, perhaps in conjunction with smoke or rate-of-rise detectors tied to a central monitoring system. Use of delays, monitoring systems such as video surveillance, and monitored door alarms can drastically reduce the consequences of false alarms and the need for officer dispatches and other responses to security breaches.

SECURITY DOORS VS. FIRE DOORS

Security and safety requirements are sometimes at odds, as airport experience with various devices has shown in connection with airport fire doors leading to the Secured Area from Sterile Areas. The problem arises when an emergency exit allows occupants to discharge into a Secured Area. Locking an emergency exit is illegal in most, if not all, jurisdictions. In many airports, delayed egress hardware has been used to restrict non-emergency exit by passengers; door releases can be delayed from 10–30 seconds to as much as 45 seconds. However, local fire codes and risk management analyses may not permit use of these devices.

CONCESSIONS AREAS

Concessions are a major source of airport revenue, and are often located throughout an airport terminal facility on both sides of security. It is usually economically advantageous for the airport to make concession areas accessible to the broadest possible range of visitors and passengers. However, enhanced security requirements suggest locating more concessions in the Sterile Areas, close to the hold rooms where only screened people are allowed, versus placing them in public areas, where persons without boarding passes can contribute to the revenue flow but may also add to congestion.

Concessions require the constant movement of personnel, merchandise, and supplies (products, foodstuffs, beverages, and money) from delivery/arrival points to the point of use or sale. Some concessionaires require intermediate food storage and processing areas within the terminal as well. Access routes for concessionaire personnel and goods should be carefully planned to facilitate authorized access.

Concessions at an airport vary in function and operational requirements. They may be as simple as a shoeshine stand, automated floral dispensing machine, or art/memorabilia display case; or as complex as a restaurant with multiple daily scheduled and unscheduled deliveries of perishables from various suppliers, and various types and locations of secure and/or refrigerated storage. Multiple security strategies are required depending upon the type and location of the concession, its delivery and storage requirements, its service circulation (trash, money-handling, high-value items such as a jewelry store,

and storage access), and its individual security requirements (duress alarms, VSS, or ATM armed guard escorts).

Due to the variety of concession types and operations, concessionaires or designated representatives should be involved early in the coordination process. Since concession companies and types can change with some regularity, designers are encouraged to plan flexibly. The needs of advertising concessions, cleaning contractors, and private (non-airport) maintenance and repair crews that may serve concessionaires (such as refrigeration contractors or beverage dispensing equipment) should also be considered in the overall security strategy and design.

Critical concession design and planning considerations include the ability to screen personnel and deliveries, the security ID media issuance and/or escort needs of delivery personnel, the routes of delivery and areas of access that unscreened personnel and deliveries may use, and the frequency and scheduling of that access. Since delivery personnel frequently change, and some deliveries may require armed escort (such as some deliveries of alcohol, bank/ATM papers, or mail), design considerations (access point locations and types, loading docks, phone/internet access, locations of concessions storage, and mail areas) that complement these procedural issues can minimize the security risks with proper coordination. A key security risk occurs when deliveries are escorted into the Sterile Area or other security areas and delivery persons may be left unattended or left to find their own way out. While this is a procedural problem, early coordination and planning can provide for design-related solutions such as a staffed visitor/escort sign-in/out station that requires both the escort and escorted to be present when entering and exiting. If the central accommodation for such a station is not considered in the design phase, it may be difficult to execute later on.

UNCLAIMED LUGGAGE FACILITIES

Consideration should be given for the establishment of facilities for passengers to reclaim luggage. The facilities should be in landside, as most persons reclaiming luggage do not have boarding passes to pass through the security checkpoint. Access routes for bomb squads and law enforcement agencies to the facilities should be considered.

VIP LOUNGES / HOSPITALITY SUITES

Some airports feature VIP lounges and/or airline hospitality suites, which are usually located in the Sterile Area. Access to these facilities is generally limited to paying members and elite-level frequent flyers who have passed through the security screening checkpoint. There are limited examples in the United States where the lounge provides a private entrance to the airport, dedicated TSA screening, and transportation to their aircraft.

VERTICAL ACCESS

Plans for vertical access should prevent the traveling public from accessing the airside through connecting elevators, escalators, and stairwells.

OBSERVATION DECKS

Observation decks accessed from the public area are strongly discouraged as they provide vantage points that may create security risks. Observation decks accessed from the Sterile Area present less concern, because occupants will have passed through a SSCP before accessing the observation deck. Any open-air observation decks should deny access to the AOA.

SERVICE ANIMAL RELIEF AREAS (SARA)

A SARA will often include grassy space, drinking water, cleaning capabilities such as water hoses and disposal containers, and appropriate drainage. Generally, maintenance of grassy areas is only practical

on the landside, not airside. For transiting/connecting travelers with disabilities, access to landside relief areas may not be possible due to time constraints and disability-related reasons.

In order to allow such travelers access to service animal relief, airports may choose to locate a more limited service animal relief area in the Sterile Area (for example using artificial materials and with fewer amenities), or may provide travelers with escorted access to non-designated outdoor areas for the purpose of service animal relief.

Airports should determine the need for, design, and location of a designated SARA based on the traveler markup, space and level of desired customer experience. For example, hub airports with a large connecting/transfer passenger profile will typically have a SARA in the Sterile Area in addition to the landside area.

Non-Public Operational Spaces

SERVICE CORRIDORS, STAIRWELLS, AND VERTICAL CIRCULATION

Service corridors may be desirable to enhance public aesthetics by concealing service and delivery activities, and can increase airport efficiency by providing clear, unobstructed pathways where airport personnel can quickly traverse the terminal. In the horizontal plane, service corridors may transit a portion or the entire length of the terminal. To avoid unauthorized access to Secured or Sterile Areas, service corridors should not cross area boundaries; if crossings are unavoidable, transitions should be minimized, access-controlled, and with consideration for surveillance.

Service corridors may also be used to minimize the quantity and types of security access points. If access requirements are clustered by similar personnel or tenant areas (such as airline ticket offices, concession storage areas, concessionaires, or equipment maintenance access points), a common service corridor may serve multiple entities, and may provide greater control of security than separate access points for each user.

The planning and design of service corridors should consider their placement and possible use by airport emergency personnel and law enforcement agencies. While use of service corridors by emergency personnel and LEOs is not a security requirement, proper corridor placement and design characteristics can enhance response times as well as allow for private, non-disruptive transport of injured persons or security detainees.

Public areas, Secured Areas, and Sterile Areas that are separated in the horizontal plane may overlap in the vertical plane. Vertical circulation and stairwells are more difficult to control than corridors. They provide access not only to multiple floors, but often to multiple security levels as well. In particular, fire stairs typically connect as many of the building's floors/levels as possible. Since they are located primarily to meet code separation requirements and provide egress from the facility, they are not often conveniently located with regard to security boundaries or airport operation. Thus, additional non-fire stairs, escalators, and elevators are often needed as well. Optimally, vertical cores should be shared for egress and operational movement.

AIRPORT AND TENANT ADMINISTRATIVE/PERSONNEL OFFICES

Airport, airline and tenant personnel require support space throughout the terminal for various functions. Types of personnel offices typically located within a terminal include airport administrative offices, maintenance support offices, law enforcement, ID/badging offices, security force offices and substations, and airline and tenant (including government agency) offices.

Office areas are best located close to the occupants' primary activity to minimize the need for multiple security transitions. There may be various office areas within multiple security areas depending upon the function and preferences of the airport personnel. Office areas connected via corridors and vertical circulation, to minimize the amount that the office personnel will need to cross security boundaries in their daily activities. Likewise, office spaces should be planned with consideration for visitors and public access, as well as the likelihood that those visitors might be inadvertently left unattended or unescorted, providing unintended access to security areas.

Consideration should be given where appropriate to the use of satellite police, ID, or first aid offices that allow for easy public access and the possibility of more efficient response times.

Other than the considerations of whether office areas are within security areas and how frequently office personnel will cross security boundaries, the security of the office areas themselves is often an anti-theft and personal safety concern. When airport operator/administration offices are located within a public terminal, these areas are often equipped with security access control equipment and/or monitored by surveillance cameras or patrols. It is typically more cost-effective and efficient to use a single security system for all requirements; these areas usually require security door treatments, duress alarms, and connection to the airport operations center and monitoring equipment.

Additional security design considerations include airport personnel and financial records, access control and ID workstations, ID media stock and records, safe and money-storage areas, and computer server and IT/communications equipment areas, especially for security-related systems such as access control and VSS.

TENANT SPACES

There is no fixed rule on whether tenant spaces require tie-in to the ACS. There are currently no such regulatory requirements for tenants to have a security program, although if the airport requires an ACS in tenant areas, it is wise to design a single system rather than try to integrate multiple tenant systems. This decision necessitates early discussions with each tenant, and perhaps a representative of the tenant community as a whole, to look at such protection requirements as money-handling operations, high-value cargo, overnight cargo and maintenance operations, and late night or early morning concession deliveries.

PUBLIC SAFETY OR POLICE OFFICES

Office space for airport security or law enforcement personnel should be provided in or near the terminal building and be sized after thorough discussions with police. Access to police facilities in the terminal complex should allow public entry into a controlled meeting area to mitigate the effect of a detonated device and/or small arms fire. This might include use of ballistic materials, window laminates, and concrete bollards/planters to prevent vehicular penetration.

Satellite police facilities can be distributed throughout multiple terminal locations to improve response times, as well as reduce vulnerability to a single point of attack.

Adequate space should be considered for:

- Communications
- Surveillance monitoring
- IT systems
- Briefing/work room
- Training classroom/offices

- Property/evidence room(s)
- Conference rooms
- CP/operations room(s)
- Holding cell(s)
- Satellite locations, if used
- Private interrogation room
- Lockers, shower facilities
- General storage areas
- Secured arms storage
- Kitchen/lunchroom facilities

Areas requiring access for public and tenants, protected with adequate controls, include:

- Administrative offices
- Security ID offices
- Lost and found
- Training rooms
- EMT/medical services

Consideration should be given to electrical, fiber optic, and other utility supply and routes to and from the police areas. Special consideration should be given to additional secure communications with the National Crime Information Center (NCIC), FBI, federal task forces, and other liaisons, as well as the amounts of conduit required to accommodate future expansion in response to increasing security requirements and government liaison needs.

EXPLOSIVES DETECTION CANINE (K-9) TEAMS AND FACILITIES

When an airport has K-9 teams in residence, appropriate accommodations for the dogs and handlers must be provided. Design is dependent to some degree on local weather conditions, the number of dogs, and the layout of the airport. If there is no on-site K-9 operation but the airport has on-call access to teams from other jurisdictions for emergencies, it would be prudent to specify a non-critical area that could be easily converted for temporary visiting K-9 use.

There are no specific technical requirements for dog accommodations, but a good rule of thumb is a 4-foot by 8-foot indoor pen per dog, attached to an outdoor, fenced exercise run. Plumbing and drainage is important; the concrete floor can be epoxy-coated for ease of cleaning. Fresh air circulation is also important, as is a dry environment, without mildew or other dampness that can affect a dog's health and sensory abilities.

The investment in dogs and their training is substantial; their area should be secured, and sufficiently isolated from casual public contact. A separate room for veterinarian services should also be provided for health care, grooming, etc.

The primary consideration is to provide a relatively normal canine housing environment. Dogs spend the majority of their time either waiting for an assignment or in training exercises. The canine environment should include an administrative area for the dogs' handlers. While a set-aside training area would also be helpful, it is common for K-9 teams to undertake training exercises in operational areas of the airport

such as parking lots, cargo ramps, baggage make-up, and bag claim areas, to maintain a realistic training environment. The designer should consider at a minimum:

- Areas should have adequate ventilation, cooling, heating, and sanitation systems.
- Areas should provide isolation from jet fuel fumes, since the dog's sense of smell is critical to its mission.
- Kennels must not be located near runways, taxiways, engine test cells, small arms ranges, or other areas where the time-weighted overall average sound pressure level for any 24-hour period exceeds 75 adjusted decibels.
- Areas should be free of infestations of mosquitoes, ticks, rodents, or other pests.
- Areas should allow for the proper supervision, protection, and care of the canine.
- Administrative areas should have secured storage for training items such as luggage, K-9 supplies, etc.
- Storage facilities must be provided for explosives training aids, which must be coordinated with the TSA's National Explosives Detection Canine Team Program (NEDCTP) Office and the Department of Justice, Bureau of Alcohol, Tobacco, and Firearms and Explosives regulatory requirements, as well as the host airport's policies regarding live training aids.
- Consider areas in a reasonable proximity to bomb squad/ EOD personnel, as well as adequate parking nearby for K-9 transport vehicles.
- Additional assistance regarding kennel designs for various climates is available from the TSA NEDCTP Canine Training & Evaluations Branch.
- Law enforcement K-9 teams prefer not to co-mingle with other animals under any circumstances, if avoidable.

AIRPORT EMERGENCY COMMAND POST (CP)

In sizing the SOC and determining its equipment requirements, it is useful to consider—especially for Category X and other higher-risk airports—whether there is enough physical room, electronic accommodation, and operational capacity to handle multiple simultaneous events. For example, this might include a requirement to manage separate video and communications channels for two or more highly diverse locations having very different events with dissimilar response requirements.

A CP is a central location from which command and control of a specific activity is conducted. This facility supports an airport's Crisis Management Team during a crisis, such as a natural disaster, terrorist event, hostage situation, or aircraft disaster. The space and equipment need for a CP vary in accordance with the size, activities and resources of the individual airport. All airports should consider the importance of designating airport space for a CP, either on a fully dedicated basis or with the capability to be rapidly converted and organized as a CP, such as space in conference or meeting rooms.

FAMILY ASSISTANCE CENTER

Consideration should be given to dedicated or easily converted administrative space for use as a Family Assistance Center (FAC). The FAC should be access controlled, have adequate current and expandable communications links, provide a private and quiet environment, and include space for cots and access to restrooms. Controllable access to the FAC is particularly important to ensure the privacy of its users. See

the National Transportation Safety Board [Federal Family Assistance Plan for Aviation Disasters](#) for more information.³⁶

SECURITY OPERATIONS CENTER (SOC)

An SOC is typically the central point for all airport security monitoring and communications. Just as each airport is unique in its layout and security requirements, each airport's SOC is unique in its features, staffing, and methods of operation. SOCs are sometimes known by other names, particularly where they co-locate with other operational functions. Alternate designations may include Airport Communications Center, Airport Operations Center, or Security Control Center.

An SOC can provide multiple communications links to the airport operator including police, fire, rescue, airport operations, crash/hijack alert, off-airport emergency assistance, a secure communications channel, and liaison with federal agencies. The SOC can serve as the point of integration of all security features and subsystems of the airport security system. Complete and timely detection information can be received at the SOC and used to initiate a prioritized and semi-automated assessment and response. See section 3.3 Security Operations Center for additional details.

FEDERAL INSPECTION SERVICES (FIS)

An FIS area requires additional planning and design features to accommodate FIS-specific procedural needs. Typically, FIS facilities are located in the international arrivals building or areas, and are designed for law enforcement and security situations that are not usually encountered in domestic operations.

Since FIS requirements are almost entirely related to international air service terminals, the subject is addressed at much greater length in Appendix E: International Aviation Security.

LOADING DOCKS AND DELIVERY AREAS

Loading docks and delivery areas are very active areas at airport terminals as they are used by maintenance personnel, vendors and suppliers, delivery vehicles, service vehicles such as trash and recycling, and many others. People who use the airport loading docks and delivery areas should be provided with appropriate ID media and be subject to vehicle inspection. Consideration should be given to using a remote, consolidated distribution center, physically separated from or at the far edge of the terminal that provides the airport an opportunity to screen deliveries prior to entry to the airport. PARAS 0024 – Consolidated Receiving and Distribution Facilities, scheduled for release in early 2021,³⁷ will cover this option in more detail.

It is strongly recommended to avoid locating a loading dock adjacent to critical infrastructure and facilities (e.g., IT and communications hubs, emergency power generators, and primary emergency egress portals).

Some airports have chosen to implement off-hour deliveries to lighten truck and van traffic around the airport during the day. The loading dock area must provide access to points of delivery within the terminal, such as tenants, concessions, airlines, and airport staff. Control of this area and the people and goods being brought into the terminal facility requires a well thought-out security strategy. Depending on the locations of the dock areas and potential paths of travel to recipients, various complementary methods of in-terminal transport and security control may need to be implemented.

³⁶ For download: <https://www.hsdl.org/?view&did=484627>

³⁷ For download (when available): <https://www.sskies.org/paras/reports/>

Security risk mitigation and access control strategies should allow efficient functioning of the loading dock/delivery areas in relation to location and access to the space. Access control of doors, personnel monitoring by airport delivery recipients with ID media, screening of delivered merchandise, and video surveillance, possibly using video analytics, are all potential methods of control.

Space should be allocated and configured to allow for physical inspection of vehicles and their contents. During heightened security conditions, physical inspection, including the undercarriage, of all delivery vehicles approaching the terminal might be required, along with at least temporary vehicle inspection points and holding pens.

Another advantage of controlling vehicle access to the terminal loading dock is the reduction of unnecessary cars and vehicles that may attempt to use the loading dock area as a general temporary parking area. Vehicles left unattended adjacent to the terminal present a risk of vehicle IEDs. Video surveillance monitoring of parking areas can alert security personnel to vehicles that have been left for extended periods. Consideration should be given to parking areas that are relatively distant from the loading dock/terminal building for extended parking of service and delivery vehicles.

AIRCRAFT MAINTENANCE FACILITIES

Aircraft maintenance facilities may be located completely landside, completely airside, or as part of the airside/landside boundary line. As these facilities contain protected areas and also require public access and supply delivery, they require coordination with the airport operator for access control.

Security considerations for aircraft maintenance facility layout and placement include:

- Compliance with 49 CFR § 1542
- Prevention of unauthorized access to the aircraft, or tampering with aircraft parts and equipment
- Non-reliance on large hangar doors or openings as a security boundary/demarcation line
- Location of landside loading/delivery docks

AIRCRAFT RESCUE AND FIRE FIGHTING FACILITIES (ARFF)

ARFF stations and equipment are a requirement of 14 CFR §§ 139.315–319, which are administered by the FAA. These facilities are clearly critical to an airport's operations. The ARFF station may straddle the airside and landside boundary. Landside access may be necessary for a variety of reasons, including for public access, mutual aid responders, and for the fire fighters themselves. In a multi-station scenario, public access should be limited to the primary ARFF station, not the substation(s).

The positioning of each ARFF station must consider emergency response times and routes. Thus, stations are located for minimum response times to required locations. ARFF vehicles may also need landside access for response to landside incidents; this might include sections of frangible perimeter fencing to remote areas.

ARFF stations generally include a classroom that is often used for training and related activities. The administrative office area of an ARFF station may be open to public access, enabling persons having business with ARFF officers to enter these areas without access control. However, access to other portions of the ARFF station must be controlled to prevent unauthorized access to the airside.

FAA AIRPORT TRAFFIC CONTROL TOWER (ATCT) AND OFFICES

The FAA ATCT and its administrative offices may be located within or adjacent to a terminal complex, in either an airside or landside area. ATCT location is dependent upon runway configuration and line-of-sight criteria. ATCT security requirements should be coordinated by the airport planner and designer to

ensure that the FAA security requirements are implemented per the FAA's [ATCT Facility Design Guidelines](#).³⁸ When the ATCT is in a remote airport location, it may require significant levels of protection, being one of an airport's most critical operational facilities. Coordination between the FAA, TSA, and the airport operator is necessary in order to address all ATCT security needs and their impacts on airport operations.

FUEL FACILITIES

Fuel farms are often placed in a remote location of the airport, often with underground hydrant systems feeding fuel to the ramp areas. Security fences should surround the entire fuel farm and its above ground storage tanks; these should be access-controlled whenever possible to monitor all movements, including authorized traffic. Where distance precludes hardwiring the access control devices to the main system, there are wireless technologies as well as freestanding electronic locking mechanisms available. Video surveillance, alarms, and intrusion sensors should be considered in and around fuel farms and storage tanks to alert law enforcement and security personnel of potential intruders or tampering.

GROUND SERVICE EQUIPMENT MAINTENANCE FACILITY

Most airports maintain specialized areas for storage and maintenance of ground service equipment (e.g., baggage tugs, push-back vehicles, refueling trucks). These areas are often referred to as Ground Service Equipment Maintenance (GSEM) facilities, and may also be used to service and maintain other airport and maintenance vehicles. As with other maintenance facilities, these areas may be landside or airside, depending upon their needs and the amount and frequency of landside/airside transition.

Similar to other service and maintenance areas, particular attention should be paid to material storage and vehicle parking areas, ensuring they do not compromise airside fencing clear zones or security.

Cargo Facilities

For planning and design purposes, cargo facilities are subject to generally the same physical security requirements as any other facility on the airport, although their procedural and operational differences often require some site-specific modifications or upgrades.

The TSA is responsible for ensuring the security of cargo placed aboard passenger and all-cargo aircraft. The 9/11 Commission Act of 2007 specifically requires 100 percent screening of all cargo that is to be loaded on passenger aircraft. Part of TSA's mission is to continue to evaluate both near-term and long-term security measures, and adjust screening regimens that enable cargo screening throughout the supply chain. Although this document is primarily concerned with designated airport and airline facilities, and secure areas of freight forwarder facilities, other cargo shippers that are certified to tender screened cargo to air carriers can also apply these guidelines.

TSA has adopted security measures throughout the air cargo supply chain that apply to aircraft operators, foreign air carriers, indirect air carriers (freight forwarders), and participants in the Certified Cargo Screening Program (CCSP). Under CCSP, shippers and other entities are allowed to screen cargo at an earlier point in the cargo supply chain, which also has an impact on the planning and design of cargo facilities both on and off the airport. Early coordination with all stakeholders of facilities where air cargo is sorted, screened, or loaded onto pallets or containers is necessary to ensure that security requirements are addressed.

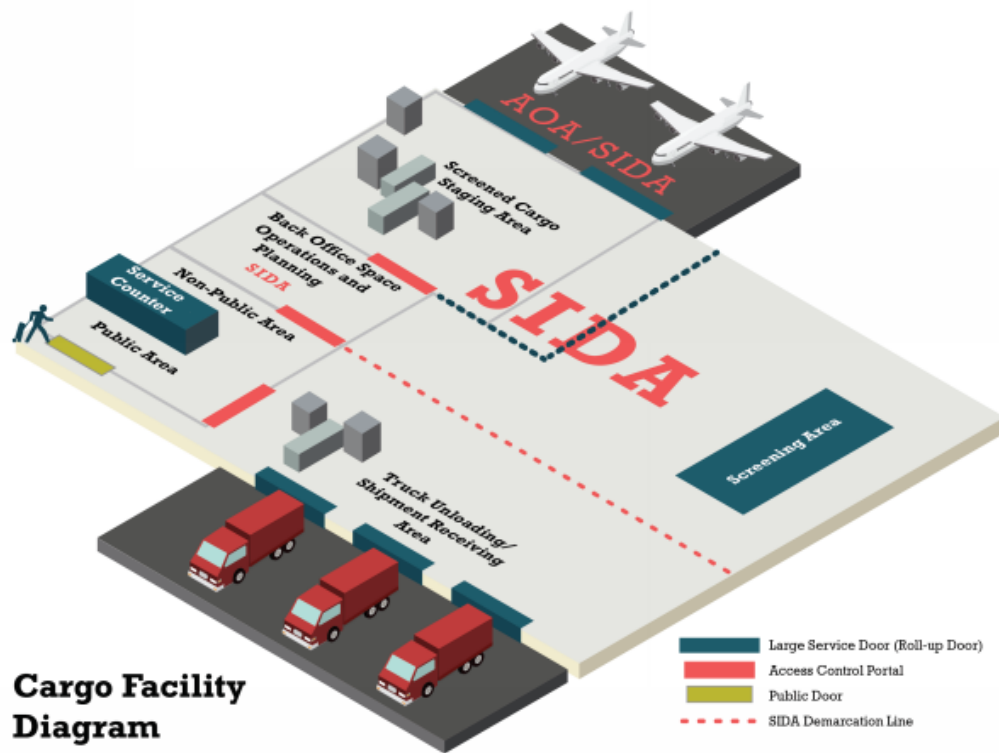
³⁸ For download: <https://www.faa.gov/documentlibrary/media/order/6480.7d.pdf>

About 50,000 tons of air cargo is shipped in the United States daily, and of that amount, about one quarter is shipped via domestic passenger air carriers. Thus, given the continuing threats against the aviation sector and air cargo itself, the security considerations during planning and design of cargo facilities are important, as well as varied and complex. The principal considerations revolve around a facility’s location and the type of business operating from that facility. In general, there are three types of cargo businesses/facilities: those accepting and processing cargo that will be transported in passenger aircraft; those accepting and processing cargo that will be transported in all-cargo aircraft (freighters); and those accepting both types of cargo. To meet the screening requirement, another type of cargo facility has evolved from the implementation of the CCSP—the Independent Cargo Screening Facility, which is now an option for shippers to screen cargo before tendering the shipment to an air carrier for transport.

The considerations for the establishment of a facility’s access control system and employee credentialing vary widely depending on the type of facility, the location of the facility within the airport, the size of the facility, the number of employees, the volume and type of cargo processed, the number and diversity of carriers, and the airport’s size and ASP requirements.

As shown in Figure 38, a facility usually faces an airport’s AOA/SIDA and has active portals that lead to and from the AOA/SIDA to the interior of the facility, which would require an access control program or system and an ID badging system as described in the airport operator’s ASP. The cargo facility’s access control system can range from something as simple as a proprietary lock and key management system to an electronic access control system that is a part of or compatible with one used by the airport operator, to conform to the airport system’s requirements. The requirements for a lock and key program should be detailed in the ASP. The ID media used could be that used by the airport operator or it could be unique to the operator of the cargo facility.

Figure 38. Cargo Facility Diagram



Landside access to a facility should be limited to a lobby and reception counter area that allows for the transaction of any business, but is separated from the rest of the facility by access controlled doors to prevent unauthorized access to administrative offices, the ramp, cargo screening areas, and screened or unscreened cargo within the warehouse. Regardless of the type of access control system, it should be scalable to allow for upgrades.

There are some basic physical security similarities that cargo facilities share when located on any airport property. These include the establishment and support of a perimeter around the facility, access control and credentialing protocols for employees, and lighting and video surveillance of the facility.

Cargo Facility Design Checklist

- Cargo facility perimeter
 - Fence/boundary consistent with ASP
 - Access control and monitoring
 - Appropriate lighting and video surveillance
 - Public access limited
 - Scalable to allow for upgrades
- Storage and screening
 - Secure storage space for unscreened cargo
 - Cargo segregation based on screening progress
 - Secure storage for high value, perishable goods
- Video surveillance locations include:
 - Public-side loading dock
 - Customer service counter
 - Cargo screening areas
 - Staging areas
 - Non-public ramp area
 - All access doors to AOA/SIDA
 - Public and employee parking areas