PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0004

April 2017

Recommended Security Guidelines for Airport Planning, Design, and Construction

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

TranSecure, Inc.
Olney, MD

COPYRIGHT INFORMATION

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 Airport Security Systems Integrated Support Testing (ASSIST) 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 Program for Applied Research in Airport Security (PARAS), 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 for proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

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

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies Special Programs Manager*

PARAS 0004 PROJECT PANEL

Lydia Bearisto *General Mitchell Milwaukee International Airport*

Michael Duffy *Transportation Security Administration*

Lorena de Rodriguez *Safety and Security Instruction, Inc.*

Chris Runde *American Association of Airport Executives*

Theresia Schatz *Airport Cooperation Research Program*

T. J. Schultz *Airport Consultants Council*

Larry Studdiford *Studdiford Technical Solutions, LLC*

CONTENTS

TABLES & FIGURES

SUMMARY

This document represents the fifth 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 now provided by National Safe Skies Alliance in 2017. All have had extensive participation in and contributions of content 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.

The Guidelines are not government regulations and requirements; they are a compendium of real-world experience and best practices developed by outstanding professionals in the field, providing recommendations for airport security–specific planning and design concepts that are scalable to airports of any size and complexity. The document takes the reader from the initial development of the airport's requirements in the Concept of Operations process through every element of an airport's security systems, including physical layout, perimeters, access control, communications, IT systems, surveillance, terminals, airside/landside considerations, and the command and control center where all the security functions come together. Further, the Guidelines document provides hyperlinks to external resources that give the reader a wide range of in-depth technical and operational detail.

PARAS ACRONYMS & ABBREVIATIONS

The following acronyms and abbreviations are used without definitions in PARAS publications:

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
ANSI	American National Standards Institute
AOA	Air Operations Area
ARFF	Aircraft Rescue and Firefighting
CCTV	Closed Circuit Television
CDC	Centers for Disease Control and Prevention
CD/DVD	Compact Disc/Digital Video Disc
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
ID	Identification
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
R&D	Research and Development
ROI	Return on Investment
SIDA	Security Identification Display Area

SOP	Standard Operating Procedure
SSI	Sensitive Security Information
SSN	Social Security Number
TCP/IP	Transmission Control Protocol/Internet Protocol
TSA	Transportation Security Administration
XML	Extensible Markup Language

SECTION 1: SETTING THE STAGE

1.1 Introduction

Integrating security systems and operations into the planning and design of airport construction and refurbishment projects can be a very complex task. The term “security system” covers a broad range of equipment, technologies, procedures, and operational approaches that need clear and concise guidelines. The task is further complicated by an environment of evolving threats, often accompanied by the implementation of new legal or regulatory requirements and operational updates to counter the changing threat conditions. Finally, security systems are inherently difficult to plan, design, and implement when applied to airports, which are designed to facilitate the fast and efficient movement of customers and goods.

Airports tend to be in a constant state of change in terms of their physical layouts, operations, and tenants. Even as the industry has seen significant mergers of domestic and international airlines, new, alternative carriers are entering the market. And while the number of new airports being built is relatively small, many airports and terminals are being remodeled, expanded, and upgraded. The majority of changing security requirements will be accomplished in existing facilities that are often decades old, designed at a time when the threat profile and the security environment were dramatically less stringent than they are today.

All of these points emphasize that there is not a single, one-size-fits-all solution to the unique problems encountered at each airport when designing and integrating security systems, nor is there a single planning and design approach for the physical space and facilities that can be universally applied to all airports.

This publication is intended to help mitigate these challenges, by focusing on various security planning and design issues surrounding airside, landside, terminal, perimeter, IT, surveillance, access control, and the unsecured but critical publicly accessible side of the airport. This guidance contains no legal or regulatory mandates, but the guidance document itself is required by 49 U.S.C. § 44914 (1990). The planning and design concepts are current to late 2016.

This document consolidates information developed through the participation of professionals from the TSA; other government agencies; and aviation, airport, and related industries. The information contained herein represents a broad range of aviation security programs and projects at numerous U.S. airports, and the continuing efforts of government and industry to develop improved approaches to incorporating effective, less costly security features into the early planning and design stages of airport facilities improvements. This version is the fifth update since the series was initiated by the FAA and adopted by the TSA; this document has been revised and updated periodically as lessons are learned, and laws, regulations, security requirements, and technologies have changed. The modifications found in this iteration are most extensive in the sections regarding baggage screening systems, passenger screening checkpoints, and access control systems, including biometrics, all of which have experienced significant changes in recent years. There is also new material addressing command and control facilities and development of a concept of operations (ConOps) due to the growing complexity of airport security systems.

In response to the September 11, 2001, terrorist attacks in the United States, and with the potential for future attacks, the President signed into law the Aviation and Transportation Security Act (ATSA) on November 19, 2001. The creation of the DHS by the Homeland Security Act of 2002 realigned a patchwork of government activities into a single department with the primary mission to protect our homeland, resulting in the most significant transformation of the U.S. government since World War II.

There are numerous advantages to incorporating security concerns into the airport planning and design process at the earliest phases of planning and development. Timely consideration of such needs will result in less obtrusive, less costly, and more effective and efficient security systems. Such systems are less likely to provoke passenger complaints or employee resistance, and are more able to fully meet regulatory and operational requirements. Proper planning can also result in reduced manpower requirements and consequential reductions in airport and aircraft operator overhead expenses.

Careful review of the prevalent threat environment, and applicable security standards and countermeasures prior to finalization of construction plans, will help determine an airport's most appropriate security posture. Such a review may also help to reduce reliance on labor-intensive procedures and equipment, which is common when an airport is required to quickly retrofit security. Inclusion of security experts early in the planning process will result in a better coordinated and more cost-effective approach to security.

This security guidelines document is intended to help the user ensure that security considerations and requirements are a significant component of the planning and design of airport infrastructure, facilities, and operational improvements.

1.2 Applicability

These recommended guidelines are provided for consideration by airport operators, airport planners and 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 considerations and coordination, since any airport project's successful conclusion will have physical and procedural security consequences. In addition, the ConOps process provided in this document should be considered when performing assessments of airport security threats and vulnerabilities, as required by 49 U.S.C. §§ 44903, 44904, 44914, and 44916, and when considering applications for grants under § 44923.

Portions of this document outline procedural aspects of operational processes, extending beyond the proposed 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. It is hoped that this document will facilitate meaningful discussion between designers, airport operators, security experts, and the aircraft operators on ways to meet security requirements in a cost-effective manner.

This document provides guidelines and recommendations only. It is not intended to suggest mandatory measures for any U.S. airport. Although this document contains information primarily of interest to commercial airports regulated under 49 CFR § 1542, some suggestions may be useful for consideration by general aviation (GA) airport operators as well. GA airport operators may also refer to a document developed by a joint TSA-industry working group in 2004, entitled *Security Guidelines for General Aviation Airports*, which is still available on several websites.

1.3 Purpose

The purpose of this document is to provide guidance for professionals responsible for, and affected by, the integration of security considerations into the planning and design of airport facilities during construction or refurbishment. This includes security design professionals as well as architects and other design professionals. Use of this document at the start of the airport planning and design process helps ensure that security needs are adequately considered.

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. Security features that have been factored into initial airport facility design are more likely to be cost-effective, better integrated, and more operationally useful than those superimposed on existing structures through add-ons, and change orders, Likewise, security features that have been coordinated early in the planning and design process with FAA, TSA, and other concerned agencies, as well as with airport tenants (e.g., airlines and other aircraft operators, ground handlers, repair stations, catering, and concessions), and end users (e.g., law enforcement, public safety and regulatory agencies, and airport operations and maintenance personnel) through a cooperative ConOps process are more likely to be well-received and operationally successful.

Essential considerations include:

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

These guidelines also identify airport areas requiring special attention in the planning process, and are intended to result in systems that will not hamper operations, cause undue economic burdens, or turn airports into armed fortresses. At the same time, the guidelines must not be interpreted to mandate specific requirements to be met by any airport operator, large or small. They may suggest numerous alternate solutions to any security challenge. Architects, planners, and designers are urged to examine and consider all potential avenues before selecting the solution that best addresses their airport's unique needs and operational environment in a responsive and cost-effective manner.

Users of these guidelines are reminded that the installation of 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.

This document is designed to be used primarily in digital/electronic PDF format, although it is also easily used by hard copy readers. In the electronic PDF version, listings in the Table of Contents, or any other link in the body of the text, are hyperlinked; simply click on the title heading or link and you will be taken to that section of the document.

Within the body of text, you will also find hyperlinked text referring the reader to other related sections, topics, and graphics within the document. For example, where unique terminology is not clearly defined when used in the text for the first time, or where reference to a more complete definition is deemed useful, a hyperlink is provided to Abbreviations, Acronyms, Initialisms and Symbols. Similarly, there are links to relevant external resources and internet websites, such as regulatory references, government and industry publications and reports, and technical standards. These links will take the reader to the complete list in this document's bibliography, where links can be followed to the internet source at the reader's convenience.

1.4 Background

The Aviation Security Improvement Act of 1990[1] directed the FAA to develop guidelines for airport design and construction, in consultation with airport operators, air carriers, and other appropriate experts, to take security enhancements and improvements 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 did not accommodate the application of appropriate security measures at that time. The requirement for these guidelines was codified in 49 USC § 44914, and a later act added the requirement to consider the results of threat and vulnerability assessments performed under § 44904 when drafting these guidelines.

The Aviation and Transportation Security Act of 2001 (ATSA)[2] 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 TSA were defined further in 2002 with the passage of the Homeland Security Act[3], which created DHS. The primary missions of DHS include preventing terrorist attacks within the United States, reducing the United States' vulnerability to terrorism at home, 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 law: information analysis and infrastructure protection; chemical, biological, radiological, nuclear (CBRN), and related

[1] PL 101–604
[2] PL 107–71
[3] PL 107–296

countermeasures; border and transportation security; emergency preparedness and response; and coordination with other parts of the federal government, with state and local governments, and with 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 threat and vulnerability assessments, risk management, flow modeling, and bomb 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 2015[4] 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 in 2013.[5] The Transportation Security Acquisition Reform Act of 2014[6], 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.

1.5 Coordination

For new construction or extensive renovation, airport facility planners and designers should encourage the 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, local emergency response personnel, and aviation security and other regulatory officials. Its role is to assist planners and designers in factoring the appropriate security and safety perspectives into plans and designs for construction and refurbishment, and to accommodate anticipated long-term expansion and regulatory changes where possible. This is captured in the development of a ConOps, 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 TSA 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, past history of criminal/violent activities likely to impact airport security and operations, and could include recommended countermeasures.

[4] PL 114–4

[5] See also Congressional Research Service (CRS) DHS Appropriations Report R43796

[6] PL 113–245

Careful attention must be given to coordination with the regulatory requirements found in 49 CFR §§ 1540 and 1542, and the sometimes overlapping areas of control and managerial jurisdiction spelled out in each airport's required site-specific Airport Security Program (ASP).[7]

Careful consideration should be given to the needs of law enforcement, security, and safety support personnel during airport facility planning, design, or renovation. 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 U.S. Federal Inspection Service (FIS) agencies.

The needs of FIS agencies—e.g., DHS Customs and Border Protection (CBP), U.S. Fish and Wildlife Service (FWS), and Public Health Service (PHS)—operating at U.S. airports are addressed in the CBP *Airport Technical Design Standards* for Passenger Processing Facilities, in separate FWS and PHS standards, and in parallel industry and National Safe Skies Alliance documents. These discuss the physical characteristics of the FIS area, and set requirements for the design of new or remodeled airport terminal building facilities for CBP processing of international passengers and their luggage arriving in the United States.

The CBP *Airport Technical Design Standards* also discuss passenger and baggage flow and 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. The CBP periodically updates the CBP Design Standards to include unified passenger processing, preclearance facilities, GA facilities, and other facility requirements.

The reader should refer to the most current CBP standards when accommodating those agencies' requirements while preparing a design for an airport project.

1.6 Changing Security Concerns and Contingency Measures

Airport planners and designers are encouraged to consider the potential impact that changing security concerns, as well as security and safety contingency measures, can have on airport facility design. Planners and designers should consult with airport security coordinators, airport operators, aircraft operators, TSA security officials, other agency officials, and the FAA's representatives at the airport to ensure that designs facilitate the implementation of local airport and aircraft operators' (including foreign air carriers') contingency-measure requirements.

Airport operators, in consultation with their FSD, must develop and incorporate into their TSA-approved ASP an Aviation Security (AVSEC) Contingency Plan that is tailored to the airport. AVSEC systems, methods, and procedures address specific types of potential security events. In developing the plan, the airport operator and FSD should consider the relative risk to the airport, existing vulnerabilities identified through a vulnerability assessment of the airport, unique characteristics of the airport, and resources available to the airport operator to undertake a response and recovery effort.

The Gerardo Hernandez Airport Security Act of 2015[8] addresses security incident response at airports. It 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

[7] See 49 USC §§ 44903(c)
[8] PL 114–50

enforcement officer (LEO) response, and joint exercises and training at airports. The resultant plans and actions could be taken into account during airport construction or refurbishment, perhaps to create or move LEO offices closer to checkpoints, or arrange for multipurpose rooms and spaces for evacuation staging areas and incident response training.

When the Secretary of Homeland Security declares an alert, the airport operator and others will implement the corresponding security measures contained in the AVSEC Contingency Plan and all appropriate security directives.

In addition, the airport operator will coordinate portions of the FAA-approved Airport Emergency Plan (AEP) with the TSA FSD. The AEP will identify the local emergency response agencies (e.g., hospitals, emergency medical services, mutual-aid first responders, military and federal support agencies), and the types of services to be accommodated, and may require additional or alternative uses of airport facilities during emergency conditions.

It is essential to approach security designs with flexibility and change in mind. As security technologies improve, threat profiles change, and security regulations and requirements are adjusted, security systems will continue to evolve and adapt. Just as early planning can save costs and effort in a project, so can planning for flexibility and change.

Recent examples of changing security concerns include the installation of advanced security equipment and exit lane security. TSA published a Final Rule on Passenger Screening Using Advanced Imaging Technology on March 3, 2016. The final rule amends civil aviation security regulations at 49 CFR § 1540.107 to allow the use of advanced imaging technology (AIT) for the screening and inspection of an individual for metallic and non-metallic weapons, explosives, and dangerous articles concealed under layers of clothing prior to entering the Sterile Area of an airport or an aircraft. More widespread installation of this technology by TSA could encourage use of these recommended guidelines should an airport operator, in coordination with TSA, plan to make changes to an airport's facilities, change the layout at security screening checkpoints, or adjust the checkpoint power supply.

The Bipartisan Budget Act of 2013[9] raised the amount passengers pay for security services, repealed the amount U.S. and foreign airlines had to pay, and gave TSA the "responsibility for monitoring passenger exit points from the Sterile Areas of airports," which was about 355 of 956 exit lanes nationwide. Funds were provided to establish technology pilots to evaluate the effectiveness of exit lane technologies, which are currently being tested or used at several U.S. airports.

1.7 Checklists

Purpose Checklist

□ Develop a ConOps to Identify Key Concerns & User Requirements
- Restrict access to security areas
- Control the flow of people
- Ensure efficient screening
- Protect vulnerable areas & assets
- Protect aircraft, people & property
- Blast mitigation measures

[9] PL 113–67

  - ▪ Space for EDS & ETD devices
  - ▪ Space for EOD operations
  - ▪ Space for law enforcement

□ Identify Early Coordination Needs

  - ▪ Airport LEOs
  - ▪ Emergency Response Agencies
  - ▪ Fire Code Officials
  - ▪ Building Code Officials
  - ▪ Model Code Officials
  - ▪ Operations/Maintenance
  - ▪ Other End Users

Coordination Checklist

□ Initial coordination with the TSA FSD

□ Get the early involvement of Airport Security Committee and others

□ Ensure 49 CFR and ASP requirements are met

□ Consider the needs of law enforcement, emergency response, security and safety support

□ Reference CBP *Airport Technical Design Standards* at airports where FIS areas are involved

SECTION 2: INITIAL PLANNING AND DESIGN CONSIDERATIONS

2.1 General

General planning, design, construction, and operational requirements of a commercial airport are established and overseen by the FAA under airport certification requirements identified in 14 CFR § 139. 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 specific 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.

The FSD is the designated TSA official who approves the required Airport Security Program (ASP) document, which identifies how the airport will meet security requirements established by regulations as defined in 49 CFR § 1542. The FSD and local FAA Airports Division officials are directly involved with the airport operator, and should be consulted during all phases of any project that affects security.

FAA regulations also require airport operators to integrate a Safety Management System process into their overall safety program. This requires airports to establish hazard reporting systems, a risk assessment process, and a risk mitigation and assurance process with the participation of airport management. Significant changes in airport facilities or procedures and overall security concerns could be impacted.

Planning for security must be an integral part of any design project undertaken at an airport, including physical structures and IT systems, among others. The most efficient and cost-effective method of instituting security measures in any facility or operation is through planning and analysis at the start of the design process, supported by monitoring and amendment of those analyses, if required, throughout the project. Selecting, constructing, or modifying a facility without considering the security implications for the protection of the general public, the facility, passengers, and airport and air carrier personnel can result in increased risk to persons and assets, as well as have a costly impact on facility modifications, or cause project delays.

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). At a minimum, a physical security approach should include:

- A vulnerability assessment, which includes a confirmation of regulatory compliance (see Appendix A) to evaluate the existing security at an operational airport, or development of a comprehensive security plan that evaluates the potential vulnerabilities at a new facility or site.
- A Concept of Operations (ConOps) plan that considers the physical and operational needs of all users, and outlines the proposed approaches to planning, design, and integration to meet those requirements. A properly developed ConOps establishes the framework for coordination of all that follows. ConOps is discussed in greater detail in Section III.
- Periodic inspections to ascertain whether a security program and its implementation meet pertinent federal, state, and local standards or regulations.
- A comprehensive ongoing security and threat awareness program to gain the interest, support, and participation of employees, contractors, consultants, and visitors.
- Procedures for implementation that include immediate, positive, and orderly action to safeguard life and assets during an emergency. This will be accomplished primarily through the 14 CFR §

139.325 FAA-required Airport Emergency Plan, coordinated with airport security contingency measures.

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

2.2 Facility Protection

The airport operator has a responsibility to provide a safe and secure operating environment and infrastructure. The extent of necessary facility protection should be examined by the local Airport Security Committee, based on the results of a comprehensive security assessment of the existing facility. High priority should be placed on protection of the aircraft from the unlawful introduction of weapons, explosives, or dangerous substances. Refer to Appendix A, Airport Vulnerability Assessment Process for further information.

Perimeter protection (e.g., fences, gates, and patrols) is the first line of defense in providing *physical* security for personnel and property at a facility. Some more advanced technologies can reach outside the fence to identify approaching threats, or may be used in an environment where there is no fence or physical barrier, such as a water boundary or swamp.

The second line of defense, and perhaps the most important, is interior controls (e.g., access control and checkpoints). The monetary value and criticality of the items and areas to be protected, the perceived threat, the vulnerability of the facility, and the cost of the controls necessary to reduce that vulnerability, will determine the extent of interior controls.

2.3 Planning and Facility Protection

The primary objective of facility protection planning is to ensure both the integrity and continuity of operations, and the security of assets.

2.3.1 General Security Areas and Boundaries

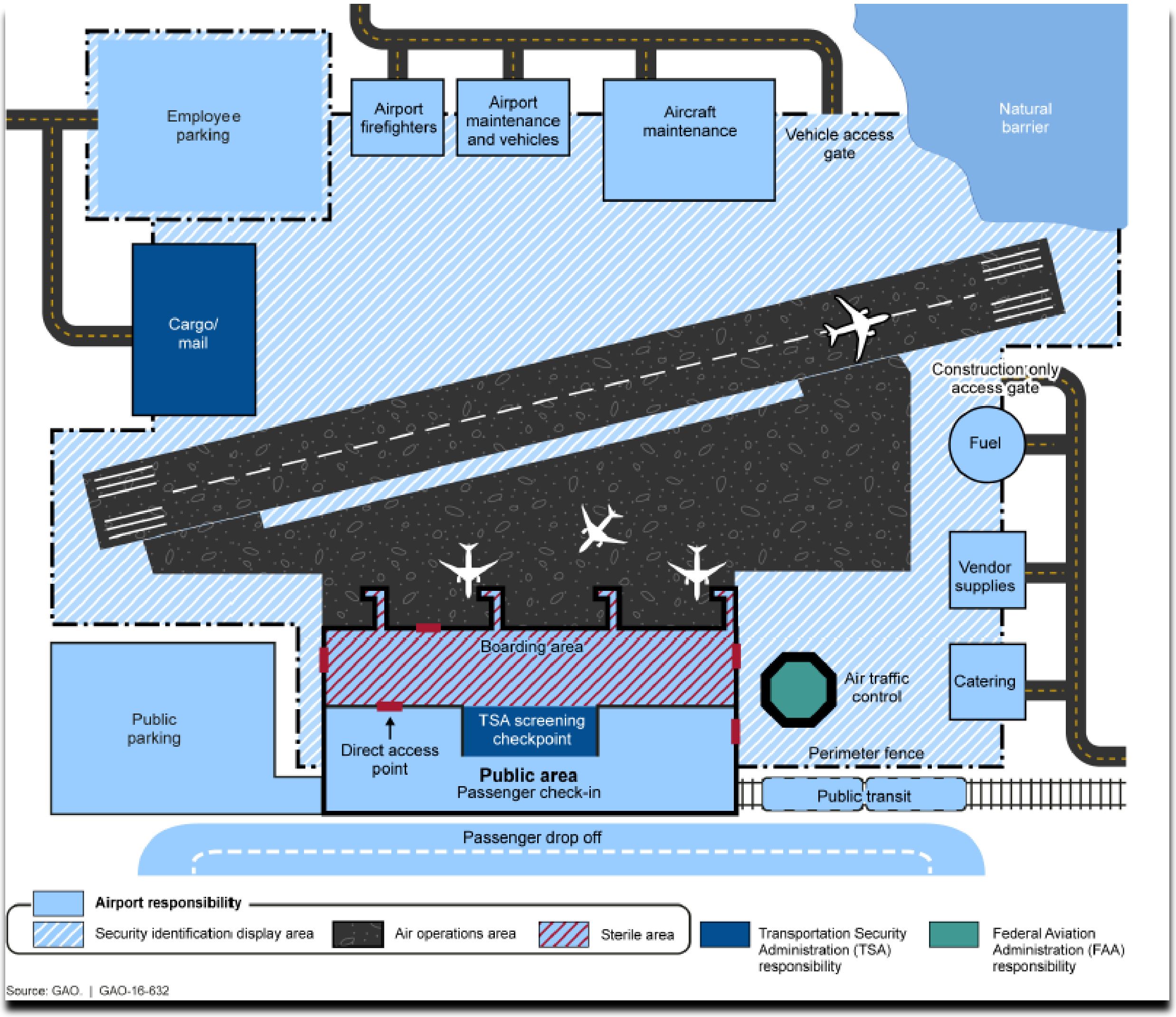
Several components of airport operations should be considered when planning for the protection of an airport facility. Figure 2-1 is a generic depiction of the various security-related areas at a typical commercial airport, such as a terminal, aircraft apron, runways or taxiways, and other components 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 a particular airport. 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, however, 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 simply geographic coordinates. The distinctions between these 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 Areas Basic Requirements: Table 2-1 provides general comparative descriptions and regulatory requirements (including training, criminal history records checks [CHRC], and identification [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 airport security coordinator and FSD for further localized definitions at the airport.

  Note: Some designers use the term, “Restricted Area.” This is a broad generic term and does not carry a specific definition in U.S. airport security regulations; however, it may be used locally to describe other areas of non-public concern, such as administrative offices, supply rooms, telecomm closets, etc.

Figure 2-1. Security Areas General Depiction



Source: GAO. | GAO-16-632

Table 2-1. Security Areas—Basic Requirements and Descriptions

	Secured Area	SIDA	AOA	Sterile Area
Regulatory Requirements	1. Access controls meeting 49 CFR § 1542.207 2. Security training 3. Full CHRC and TSA Security Threat Assessment (STA) 4. ID display/challenge	1. No access controls required by regulations 2. Security training 3. Full CHRC and TSA Security Threat Assessment (STA) 4. ID display/challenge	1. Basic access controls meeting 49 CFR § 1542 2. Provide security information 3. STA required	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.

Source: TranSecure, Inc.

2.3.2 Vulnerability Assessment

In order to implement security at an airport, it is necessary to understand and quantify the degrees of security into three key issues:

1. What is the threat to the airport?
2. What is an airport’s level of vulnerability relative to each element of that threat?
3. To what extent is the threat/vulnerability likely to change, and why?

A vulnerability assessment is an excellent tool and the primary means for determining the extent to which a facility may require security enhancements. It serves to bring security considerations into the mix early in the design process, which reduces the risk of a more expensive retrofit after the design or construction has begun. Many tools and methodologies are available; all are subjective to varying degrees, largely because, in every case, one must first have a thorough understanding of both short- and long-term threats in order to understand and respond to the three key issues noted above. With this in mind, the planning and design team's response to these points will be a recommendation of a combination of security measures, both physical and procedural, to provide enhanced security and ease of movement for both passengers and employees. Refer to Appendix A, for further information.

2.3.3 Protection Criteria

The Airport Security Committee may offer recommendations that consider the following:

- Known threat(s) specific to the airport and/or to the airlines serving it
- History of criminal or disruptive incidents in the area surrounding the facility, but not primarily directed toward airport operations
- Domestic and international threats and the general integrity of the U.S. transportation system
- Facility location, size, and configuration
- Extent of exterior lighting
- Presence of physical barriers
- Presence of access control and alarm monitoring systems, closed-circuit television systems, and other electronic monitoring systems
- Presence and capabilities of onsite staff, law enforcement, and/or security patrols
- Other locally determined pertinent factors, such as general aviation, commercial operations, and intermodal transportation facilities

2.3.4 Physical Protection

Airport and aircraft operators provide protection through a combination of mobile patrols or fixed posts staffed by police, other security officers, or contract uniformed personnel; security systems and devices; lockable building entrances and gates; and cooperation of local law enforcement agencies. The degree of normal and special protection is determined by completion of a vulnerability assessment and a crime prevention assessment.

2.3.5 Crime Prevention

The local police department may collect and compile information about criminal activity on or against property under the control of the airport, provide crime prevention information programs to the occupant and federal agencies upon request, and conduct crime prevention assessments in cooperation with appropriate law enforcement agencies.

2.3.6 Recordkeeping

In addition to physical protection, airport operators also need to keep records of incidents, personnel access, or other activities. Some of the records (such as personnel access) may be collected automatically. Recordkeeping needs, including some video applications, may affect IT systems, cable designs, and equipment locations, as well as require secure data storage. These needs should be coordinated early in the design process.

2.3.7 Delegations of Responsibility

Some security responsibilities under 49 CFR § 1542 may be transferred to a tenant or aircraft operator. Normally, the airport operator will retain responsibility for enforcement, monitoring of alarms, requests for criminal investigations, and fire, safety, and health inspections. This type of agreement between airport and aircraft operators is known as an Exclusive Area Agreement, or in the case of other airport tenants, an Airport Tenant Security Program. There may also be letters of understanding among nearby jurisdictions to provide assistance to each other during emergencies, but in most instances, these are simply promises to give aid, not delegations of authority, and are sometimes conditioned on whether the other jurisdictions may have their own simultaneous emergencies underway.

2.3.8 Design Factors

It is important to consider security systems and procedures from the beginning of the design phase through completion, so that space allocation, appropriate cabinetry and furnishings, conduit runs and system wiring, heavy-duty materials, reinforcing devices, seismic requirements, and other necessary construction requirements are provided in the original plans.

Consideration of seismic requirements may seem out of place in a security guideline document. However, continuity of operations is of paramount concern in design and construction of an airport facility. For this reason, Section 4 of this document includes a brief discussion of Seismic Requirements, as similar mitigation measures may apply to a greater range of natural disasters.

2.4 Checklists

General Checklist

- □ Advance Planning
- □ Determine User Requirements in the Concept of Operations
- □ Physical Security Program
  - Vulnerability assessment
  - Periodic inspections
  - Continuing security education
  - Emergency procedures
- □ Consult with Experts in Aviation Security
- □ Coordinate with Security/Regulatory Personnel
- □ Refer to Regulatory Requirements & Standards
- □ Coordinate with TSA FSD

Facility Assessment Checklist

- □ Airport Security Committee Review
- □ Perimeter Protection – First Line of Defense
- □ Cost Analysis
  - Overall site
  - Building envelope
  - Utility systems
  - Mechanical systems (HVAC)

- □ Interior Controls
  - ▪ Plumbing / gas systems
  - ▪ Electrical systems
  - ▪ Fire alarm systems
  - ▪ Communications / IT systems
  - ▪ Security systems
  - ▪ Security Master Plan

Planning Facility Protection Checklist

- □ Ensure Integrity & Continuity of Operations
- □ Ensure the Security of Assets & Facilities
- □ Protection Criteria
  - ▪ Facility Location, Size & Configuration
  - ▪ Known Threats
  - ▪ History of Incidents
  - ▪ Amount of Lighting
  - ▪ Presence of Physical Barriers
  - ▪ Local Pertinent Factors
- □ Physical Protection
  - ▪ Mobile Patrols
  - ▪ Guard Stations
  - ▪ Security Systems
  - ▪ Lockable Access Points
  - ▪ Local Law Enforcement Support
- □ Crime Prevention
- □ Recordkeeping
- □ Delegations of Responsibility
  - ▪ Exclusive Area Agreements
  - ▪ Airport Tenant Security Programs
  - ▪ Letters of Understanding
- □ Design Factors
  - ▪ Conduit Runs
  - ▪ Architectural Conflicts

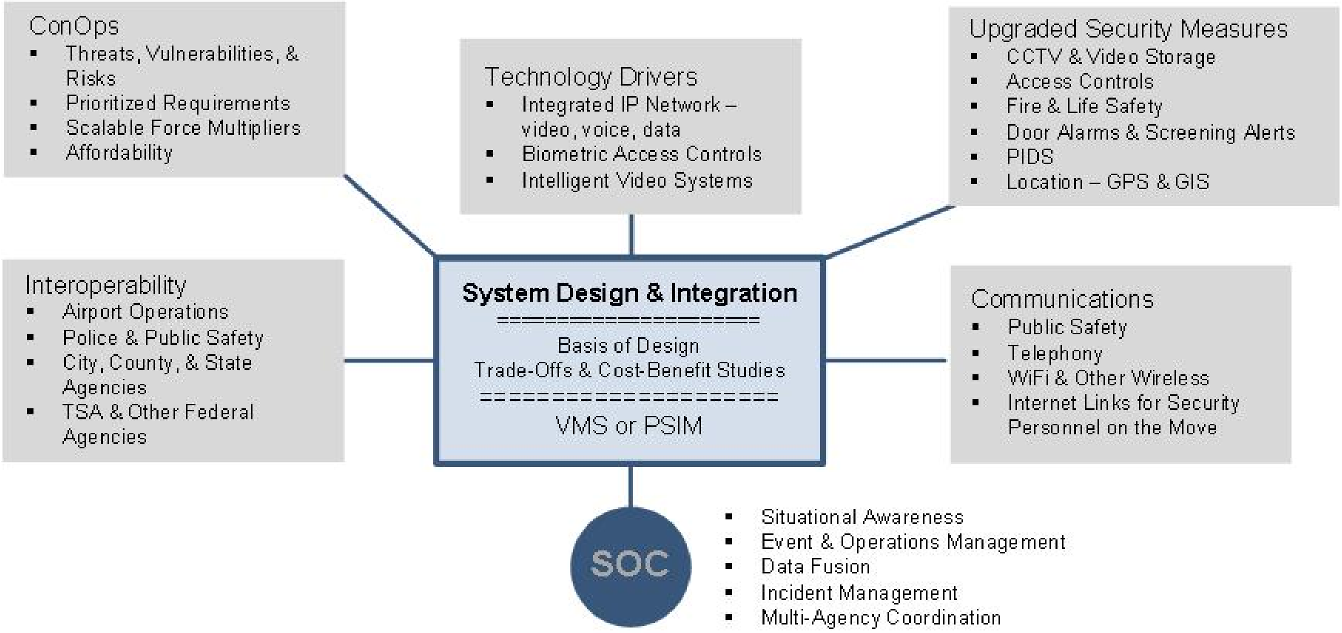
SECTION 3: DEFINING OPERATIONAL REQUIREMENTS – CONCEPT OF OPERATIONS

3.1 Introduction

The first step toward integrating security into airport planning, design, or major renovation is the analysis and determination of the airport's general security requirements. The range of available options, configurations, and functions is very broad. There is no single solution, and with very little examination, it is apparent that there are a large number of issues that must be addressed before a best approach and optimal solution can be achieved at any given airport.

The place to start is defining operational requirements, and using a Concept of Operations (ConOps) is the preferred process. Figure 3-1 illustrates the role of the ConOps in establishing operational requirements for an integrated airport physical security system.

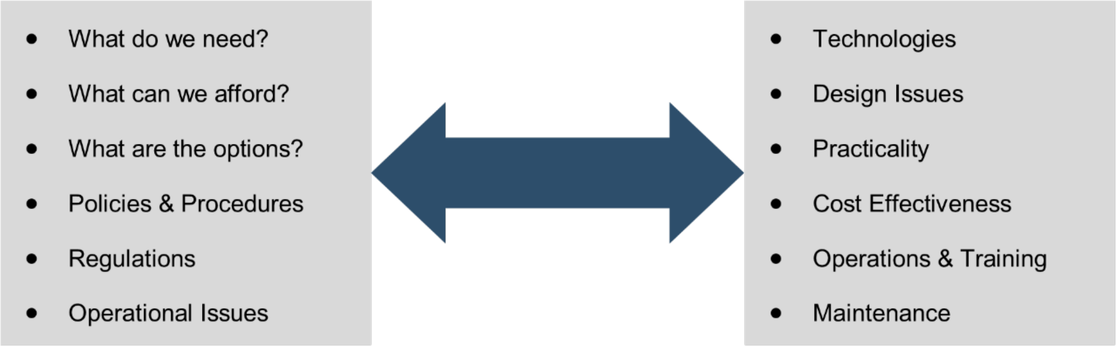
Figure 3-1. Integrated Airport Security System Development Process


ConOps
Threats, Vulnerabilities, & Risks
Prioritized Requirements
Scalable Force Multipliers
Affordability
Technology Drivers
Integrated IP Network – video, voice, data
Biometric Access Controls
Intelligent Video Systems
Upgraded Security Measures
CCTV & Video Storage
Access Controls
Fire & Life Safety
Door Alarms & Screening Alerts
PIDS
Location – GPS & GIS
Interoperability
Airport Operations
Police & Public Safety
City, County, & State Agencies
TSA & Other Federal Agencies
System Design & Integration
Basis of Design
Trade-Offs & Cost-Benefit Studies
VMS or PSIM
Communications
Public Safety
Telephony
WiFi & Other Wireless
Internet Links for Security Personnel on the Move
SOC
Situational Awareness
Event & Operations Management
Data Fusion
Incident Management
Multi-Agency Coordination

Source: TranSecure, Inc.

A ConOps is a process for developing a document that presents a high level statement of the purpose and goals of an airport security system or upgrade program, as determined by the facility's stakeholders and users. As Figure 3-2 illustrates, the process is iterative and overlaps with the design phase, so that the feedback from operational, technical, and cost trade–off studies can further refine the operational requirements. The general approach outlined here can be applied to other types of facilities as well.

Figure 3-2. The Iterative ConOps Process



- What do we need?
- What can we afford?
- What are the options?
- Policies & Procedures
- Regulations
- Operational Issues

- Technologies
- Design Issues
- Practicality
- Cost Effectiveness
- Operations & Training
- Maintenance

Source: TranSecure, Inc.

Most common views on the development of a ConOps characterize it in terms of eight basic questions:

- What does the project involve: an update of existing infrastructure, a move or expansion into new facilities, operational reorganization, new interfaces with airport departments and government agencies, or mutual aid?
- Why is this project happening? What is the impetus: system integration, physical expansion, growth forecasts, outdated technology, new regulatory requirements, inadequate or failing infrastructure, or administrative restructuring?
- Who are the users and stakeholders, both internal and external to the organization? What are their operational goals, and what information do they require?
- What infrastructure exists? What threats and vulnerabilities exist?
- Which new technologies will be most appropriate to best serve the different priorities and interactions among user groups?
- What human factors need to be accommodated, such as ergonomics, lighting and noise levels, sight lines, design factors for dealing with multiple technologies and/or multiple events, and certain staffing and training criteria?
- What is the realistic budget and where it is coming from? What are the additional related costs, such as those for staffing and long term training, operations, and maintenance?

Expanding on these questions provides the basic outline of what a ConOps should address.

3.1.1 What?

Asking the question “what?” seeks to identify the depth and breadth of security functionality to meet appropriate user requirements. What array of services is the facility expected to offer? What information is it expected to provide, to whom, and for what purposes? This can include a range of points, all needing early identification, as they will drive the detailed approaches to planning and design.

What systems and services are needed to meet the user requirements? This is limited to a high-level definition of systems in operational terms rather than in technical terms. Unless there is a specific reason for identifying details of a system, this should initially be generalized. The reasons to identify a new or upgraded system or service may include: a legacy system may exist and continue to be used (and therefore need to be identified early as a baseline condition of the ConOps); or the owner of the facility may have other operational, legal, policy, budgetary, physical space or contractual constraints that limit the ability to make changes to or replace a system. Developing a description of the appropriate level of functionality requirements will serve as the foundation for more detailed design of the systems.

The ConOps may include a preview of candidate technologies for anticipated systems in order to help describe the physical and operational parameters that will apply to, and possibly limit, further project development. Examples are discussed throughout this document.

3.1.2 Why?

This question will lead to identification of the objectives of the security system project: Why is it needed? For airport expansion and growth projections or consolidation of operational and administrative functions? For outdated or failing technologies and infrastructure, or possibly new regulatory requirements that address operational gaps and user needs? Or, perhaps, for all of the above? As a subset to this, the answer should also identify operational and administrative issues, policies, and constraints affecting the facility, which inform the planning process in determining how the project will be executed to achieve its objectives.

This emphasizes the importance of having all stakeholders engaged in development of the ConOps. The comparison and contrast of views between the executive level and the operational level should identify gaps in the objectives; identify conflicts and redundancies to be addressed and resolved; allow for the identification and resolution of differing levels of criticality and priorities; and provide a baseline for establishing near-term and long-term objectives.

3.1.3 Who?

This question addresses the identity of stakeholders, e.g., individual or organizational, internal and external to the security system and its operational elements. It should address the user requirements as classes or descriptions of users who are meaningful to the organization. In addition, it should include the operational requirements necessary for their primary responsibilities. This also begins to identify the support activities of stakeholders that arise beyond the anticipated operational activities—who owns the facility, who maintains it, who manages and pays for it—thus, also identifying persons or offices who, while not primary users, significantly influence how the project is ultimately designed and operated.

It should also provide the initial identification of the types of personnel, and the number and type of functions that will be located in the facility or interact with it in some form; identify the level and priorities of personnel or organizations that will be engaged in the process during design and development; and identify at a high level the roles and responsibilities of the stakeholders with a definition of their operational interactions, both internal and external.

For any security system, a typical stakeholder list might include the following groups:

- Management/executive staff
- Communications staff/dispatchers
- Law enforcement, contract security
- ARFF, EMTs, internal and external
- Airside operations

- Landside operations
- Curbside and ground transportation
- Airport facilities and maintenance
- Airport development / engineering
- IT
- Risk Management
- DHS, TSA, and CBP
- FAA and Air Traffic Control
- Airlines
- Concessionaires
- Tenants
- Military joint use
- Adjacent commercial/industrial parks
- Local/state/regional government
- Mutual aid
- Surrounding community

3.1.4 When?

The development of a security system may not be an isolated project; it will frequently be a part of a larger effort such as a new or renovated terminal, and have an effect on many other related activities. It is essential to have a clear but flexible schedule to allow for coordination with related programs, conflict avoidance, and incorporation of opportunities for collaboration with other projects or actions. Often, the timing may be driven by a need to meet regulatory, policy, or other procedural requirements, the nuances of which must be thoroughly understood as part of the driving force behind development. An example of this is a new or upgraded terminal expansion project that may include relocating the existing Security Operations Center and related Police and Emergency Operations facilities.

A preliminary project schedule should reflect at least the following five periods:

- Concept development period
- Pre-design phase
- Planning and design period
- Construction or implementation period, including changeover
- Useful life of the facility past construction or implementation – This element is often overlooked, but it can establish a basis for later planning for anticipated upgrades, replacement, or expansion, all of which must be reflected in long-term planning and budget considerations.

During planning and design phases, this baseline schedule will be refined and enhanced by the design team based on budgets, resource availability, project scale, and other evolving factors.

3.1.5 Where?

Addressing where to locate a new facility can become somewhat complex, especially when the facility has special requirements, or future moves, additions, or changes are planned. These can include different requirements for physical separation or proximity to another facility. For example, regulatory or operational limitations on the facility site may reflect requirements for setbacks from another area for reasons of safety or security; limits in the amount or suitability of the space (e.g., ADA requirements); infrastructure constraints; adequacy of IT capabilities in alternate locations; budget considerations; threats and vulnerabilities relative to its operations; and access requirements.

3.1.6 How?

This question addresses how the facility can be successfully developed and implemented, based on the information developed throughout the ConOps process. It includes such issues as funding, personnel, integration of existing and planned infrastructure, architectural constraints, coordination of planning and design concerns, and a list of other locally unique activities and assets to be accommodated in order for the project to move forward. The resolution of “how” is a particularly critical element of the ConOps because it establishes each sequential set of activities to be set in place for the ConOps guidance to be fully effective. This will vary depending on the particulars of each project, but, in general, should include a rough order of magnitude (ROM) of “soft” costs such as planning, design, and consulting fees required to develop the project; a similar ROM of the “hard” costs such as capital expenses for construction of facilities, IT and communications infrastructure expansion, equipment, labor, and related costs; internal and external professional resources necessary to complete and support the project, such as maintenance and training; and a proposed schedule of steps to be undertaken throughout the process, and milestones to be accomplished.

As the ConOps is developed, it provides a baseline document used to determine details such as space allocations, technology options, infrastructure support, communications requirements, and human factors affecting staffing. Further, the ConOps provides a checklist review as the facility planning and design process evolves. Periodically, the development team should review its work against the ConOps to determine if the design is meeting the objectives stated in the ConOps, and either adjust the design or revise the ConOps as necessary to accommodate the changing circumstances.

One of the reasons that many security systems may become somewhat dysfunctional is the lack of an updated ConOps, as a well as an absence of a guide for integrated development. Any significant changes affecting the facility—whether changes in technology, functionality, budget, or operational and administrative environment—should be viewed first from the perspective of an updated ConOps that looks at all of those interactions.

A considerable body of guidance literature is available for the development of a ConOps. ConOps development in professional fields other than transportation generally follows similar developmental paths, with significant variations that define dozens of possible scenarios and approaches to their resolution. For the most part, these differing approaches are not wrong; they are simply different ways of reaching the same goals. This document provides a brief outline of the resources needed, and goals to bear in mind during development.

Airport ConOps plans should be reviewed by security design professionals to harmonize with the planning and design of technology and facilities. Planners should recognize when security design cannot be adapted to ConOps requirements and make adjustments to address the design constraints.

Documents that inform development and should be considered in an airport's ConOps include the following:

- Airport Security Program (ASP): The ASP is developed pursuant to 49 CFR § 1542, which governs the overall security arrangements for the airport. It addresses matters such as perimeter security, access control, surveillance, contingency plans, and law enforcement response.
- Emergency Operations Plans: An Airport Emergency Plan for a variety of incident responses is mandated under 14 CFR § 139 and is coordinated with the ASP requirements. It is often aligned with state or local emergency operations plans where the airport may have defined responsibilities, (e.g., designation of an airport as a strategic logistics supply point in the event of an emergency, or as a strategic national stockpile distribution and reception point in the event of a pandemic).
- Incident Action Plans: A plan reflecting the overall strategy for managing certain incidents, and not necessarily requiring formal long-term planning. It may include the identification of operational resources and assignments, as well as provide management with information on the incident.

One of the goals of a ConOps is to identify operational requirements in sufficient detail to form the basis for development of a system design. The ConOps 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 ConOps should help drive the selection and design of technologies, but all too often, technologies are selected and implemented without a thorough understanding of the organization's needs. This can result in underperforming systems that are never used.

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

3.2 What a ConOps is Not

To fully understand what a ConOps is, it is equally important to understand what it is not. The nature of the document necessarily avoids definite details of operations, staffing, technology choices, and other explicit operational and design details. It seeks to identify and describe performance-oriented results and guidance, not technical specifications.

- A ConOps may generally define the type of skill sets needed in a facility, but will not define the number of people or specific tasks of individuals.
- A ConOps will describe objectives to be supported by the use of operational processes, but does not define the processes themselves.
- A ConOps may describe objectives to be supported through the use of technology and systems, and may even generally define the type of technology and systems, but it is not a detailed technical description or specification of these systems.

The ConOps will provide performance-based objectives to be met as the detailed design is worked out in concert with those objectives. The lack of specificity in technical details is intentional.

3.3 Risk Assessment

A key element of the ConOps for the development of an airport security system is a Risk Assessment, the principle components of which are a determination of threats and vulnerabilities. The standard risk formula is risk = threat x vulnerability x consequences [R= T x V x C]. In fact, a risk assessment is necessary in the general development of airports and other mission critical facilities, and should be a standard element of the early supporting activities in conjunction with the ConOps. The risk assessment can establish some starting points: what systems are in place, what changes are planned, what their strengths and vulnerabilities are with respect to a range of likely threats, and how the security planning and design process can address them in an optimal operational and cost-effective manner.

The actions taken in response to the risk assessment will often include measures designed to increase the ability of a facility to respond to an event or multiple simultaneous events, as well as provide increased safety and security measures as the irregular operations evolve. As some of these measures can increase costs for the development of the security system, it is essential that the assessment provide a clear definition of the risks and vulnerabilities to be addressed during planning and design.

The key elements of a threat and vulnerability assessment include the following:

- Develop a clear perspective of the interrelationships among the facility, the organization, and its assets. Assets include property, systems, structures, business, information/data, and people.
- Identify the threats and vulnerabilities and the risks associated with each. An outside party, preferably a party with expertise in the risk assessment process, can do this initially. The approach used by the outside party may vary from the relatively benign to the very aggressive. Regardless of the approach, the external assessment should be combined with information on the range and probability of threats and vulnerabilities known to the facility owner.
- Quantify the probabilities associated with each of the identified risks. To the greatest extent possible, the probabilities should be based on factual data. Probabilities of risk can be gathered from a range of sources, including local, state, and national agencies that have experience with events and incidents. The probabilities should include an agreed-upon scale as shown in Table 3-1.

Table 3-1. Example of a Probability Scale

Ranking	Probability of Occurrence
High	Greater than or equal to 1 in 30 (3.3%) chance in any given year
Medium	Less than 1 in 30 (3.3%) but greater than or equal to 1 in 100 (1%) chance in any given year
Low	Less than 1 in 100 (1%) but greater than or equal to 1 in 1,000 (0.1%) chance in any given year
Very Low	Less than 1 in 1,000 (0.1%) chance in any given year.

Source: TranSecure, Inc.

Once a set of risks has been identified, planners should quantify the value of losses associated with each risk. This includes financial costs, costs due to loss of use of a facility or function, cost to recover or rebuild, loss of life, loss of earnings or revenue, and loss of good will and trust. The value of a loss resulting in direct relation to the risk needs to be measured against an established system of values.

Table 3-2 is taken from FEMA guidance for an earthquake; however, the integral steps on the scale can be modified at the local level to fit a much wider range of events: what always/sometimes/rarely happens *at your airport*, and the potential effects on the facilities and infrastructure, that is, how many resources must be committed to recover to full operability. Using an earthquake as an example, depending on the vulnerability and importance of each part of the system, the amount of damage required to interrupt airport operations ranges from minor interference to a full shutdown. Some elements may fail at a relatively low level of interference; others may be able to withstand more disruption.

Table 3-2. FEMA Guidance for an Earthquake

Very small probability of experiencing damaging earthquake effects	Negligible effects
Could experience shaking of moderate intensity	Moderate shaking—Felt by all, many frightened. Some heavy furniture moved; a few instances of fallen plaster. Damage slight.
Could experience strong shaking	Strong shaking—Damage negligible in buildings of good design and construction; slight to moderate in well-built ordinary structures; considerable damage in poorly built structures.
Could experience very strong shaking	Very strong shaking—Damage slight in specially designed structures; considerable damage in ordinary substantial buildings with partial collapse. Damage great in poorly built structures.
Near major active faults capable of producing the most intense shaking.	Strongest shaking—Damage considerable in specially designed structures; frame structures thrown out of plumb. Damage great in substantial buildings, with partial collapse. Buildings shifted off foundations. Shaking intense enough to completely destroy buildings.

Source: FEMA

- Adjust the overall value of loss associated with each risk, taking into account the probability of the risk and the value of the loss.
- Quantify the organization’s ability to operationally absorb or accept a loss, and its ability and cost to recover.
- Develop mitigation plans to address the risks. Base the plan on cost-benefit and feasibility analyses.

When undertaking a risk assessment on which to base the ConOps, (See Appendix A, Risk and Vulnerability) the following issues should be considered:

- Much of the assessment cannot be easily measured or assigned a value. For example, the goodwill that any organization has, or may lose, from its customer base is difficult to measure. In some cases, opinion or emotion-based input may be unavoidable, but the assessment should be prepared as dispassionately as possible.
- A significant focus of assessments has often been on human-initiated events (criminal and terrorist activities). While this is an appropriate part of the assessment, it is only one part. The risk assessment must also consider other events, including natural disasters such as fire,

earthquake, flooding, etc., and events arising from accidents, all of which have considerable impact on design, operation, training, and staffing.

- The value of an assessment is only as good as the integrity with which it is conducted and the results are communicated. While bad news is rarely welcome, the identification of threats and vulnerabilities and the response to address them helps an organization to avoid some future degradation.

Threats and vulnerabilities change over time, as does an organization's response to both. A risk assessment, like the resulting ConOps, should not be a one-time activity, but should be revisited when experiencing major organizational, facility, or operational changes. An airport operator should not go more than five years between thorough threat and vulnerability assessments; more often if changing conditions warrant.

3.4 Situational Awareness

Situational awareness is the perception of events and activities in real or near-real time seen by an individual or group, and their understanding of how those events and activities may be related. More simply stated, it is knowing what is going on from moment to moment so that the Security Operations Center (SOC) operator can react, if required.

Situational awareness can be developed through a number of different means. It can include:

- Direct observation of an event or situation
- Observation reported by third parties
- Observation through CCTV systems
- Observation through sensing systems (e.g., fire alarms, security alarms)
- Observation related by news and media outlets

Too much information, particularly if it is irrelevant or distracting from a critical event, can be detrimental to effective decision making by the SOC operator. Excess information can place such a high demand on human operators or responders that they cannot absorb or process it all, and may miss or misinterpret critical points.

This is not to suggest that available information should be limited. An SOC should have access to information where it is appropriate and useful to decision making. Several approaches can be taken to avoid overloading the SOC without losing vital information:

- Disperse blocks of information to different people or teams, who filter critical data to a manager or team charged with decision-making.
- Establish levels of criticality for information or alarm conditions, such that more urgent concerns are elevated for attention sooner.
- Provide a smaller number of points to focus on, while allowing different information streams to be viewed. An example of this is a video wall with a limited number of screens but a high number of video feeds, allowing the SOC operator to select and change their primary views as the situation develops.

Key considerations and elements of effective situational awareness include:

- Good quality information delivered in a timely manner
- Where situational awareness drives organizational response to an event or activity, reliable bi-directional communications are essential
- Flexibility to allow for changing conditions
- The level of situational awareness required of the SOC staff drives the information sources that need to be delivered

3.5 Checklists

Define a ConOps

□ Who: Identify all users and stakeholders
□ Why: Describe the goals and objectives
□ What: Identify functionalities to meet user requirements
□ When: Devise a flexible schedule with milestones
□ Where: Consider location, space limitations
□ How: Consider all costs and capital expenses
□ ConOps provides objectives, not technical specifications

Develop a Concept of Operations

□ Identify goals and resources needed
□ Select an experienced team of experts
□ Coordinate with planning and design teams
□ Maintain good records of all decisions and actions
□ ConOps is a continuing cycle of re-evaluation over time

Risk Assessment

□ Risk considers threats, vulnerabilities and consequences
□ Conduct periodic threat assessments as conditions change
□ Consider expert assistance in periodic assessments
□ Risk can include criminal or terrorist acts, accidents, hazmat, and weather
□ Quantify the probability of occurrence for each threat
□ Quantify the value of each critical asset and recovery costs

Commonality, Scalability, and Flexibility

□ Common SOC technologies may be used for multiple applications
□ Some technologies may be available from less expensive sources
□ Choose technologies with future expansion in mind

Situational Awareness

- □ Real-time perception of events is critical for complex operations
- □ Establish SOPs for primary response responsibilities
- □ Use technology to avoid operator overload with too much information
- □ Situational awareness is knowing what is going on; situational assessment is knowing what to do about it.

Funding/Budgets

- □ Identify the source of funds, and budget accordingly
- □ Seek local government or private sector grants for funding

SECTION 4: AIRPORT LAYOUT AND BOUNDARIES

The first step in the integration of security into airport planning, design, or major renovation is the analysis and determination of the airport's general security requirements, layout, and boundaries. These decisions are critical to the efficient, safe, and secure operation of an airport. While existing airports may not have great leeway in redesigning their general layout, adjustments to the location of access roads or types of boundaries for security areas may be beneficial and integrated into adjacent construction projects. Periodic review of an airport's boundary system and locations is recommended to ensure that the airport's needs are met, particularly since aviation security requirements and surrounding environments may frequently change.

4.1 General Airport Layout

The general layout of an airport consists of three areas typically referred to by the industry as *airside*, *landside*, and *terminal*. While the terminal area generally lies on the boundary of the airside and landside (as may other buildings), due to the nature of its use and the special requirements that apply to airport terminals, it is best treated for security purposes as a distinct area.

Each major area of the airport (airside, landside, and terminal) has its own special security requirements. Airside/landside requirements and operational parameters should be carefully considered when planning and designing a new airport or facility. The requirements, barriers, and boundary measures that delineate airside from landside may have major effects on the facility's efficiency, employee and public accessibility, and overall aesthetics.

Maintaining the integrity of airside/landside boundaries plays a critical role in reducing unauthorized access to, attacks on, or the introduction of dangerous devices aboard passenger aircraft. Effective airside security relies heavily on the integrated application of physical barriers, identification and access control systems, surveillance or detection equipment, the implementation of security procedures, and efficient use of resources.

4.1.1 Airside

The airside area of an airport usually involves a complex and integrated system of pavements (runways, taxiways, and aircraft aprons), lighting, commercial operations, flight instrumentation and navigational aids, ground and air traffic control facilities, cargo operations, and other associated activities that support the operation of an airport, access to which is controlled. Annex 17 of the International Civil Aviation Organization (ICAO) founding convention covering security states the topic more simply: "the movement area of an airport, adjacent terrain and buildings or portions thereof, access to which is controlled."

Typically, the airside is beyond the security screening stations and restricting perimeters (fencing, walls or other boundaries), and includes runways, taxiways, aprons, aircraft parking, and staging areas and most facilities that service and maintain aircraft. For operational, geographic, safety, or security reasons, other facilities such as tenant and cargo facilities may be located on the protected airside as well.

The airside must be entirely nonpublic, as it generally includes security areas to which certain requirements apply under 49 CFR § 1542 (e.g., the AOA, SIDA and Secured Areas). Further information on these security requirements is contained in Section 4.2, Security Related Areas.

The choice as to where the airside perimeter fencing or barriers may be located often depends on the surrounding environment and access roads, and may be one of the most critical decisions in designing or renovating an airport. Planners should also consider the following factors as essential in determining airside boundaries and orientation:

- Dangerous or hazardous areas that could affect the safety or security of a parked or moving aircraft.
- Concealed/overgrown areas that could hide persons or objects that might endanger aircraft or critical airport systems.
- Adjacent facilities having their own security concerns and provisions, e.g., correctional, military, or other facilities that could affect or be affected by the proximity of airside operations.
- Natural features, large metal structures/buildings, or electronics facilities that might affect ground or aircraft communications or navigational systems. Reduced or limited communications can endanger not only aircraft and airport personnel safety, but also limit security response capabilities and information availability during emergency as well as routine situations.
- Adjacent schools, hotels, parks or community facilities that might affect or be affected by the proximity of aircraft and the related safety and security concerns. While safety concerns exist, the increased possibility of airside penetrations and/or vandalism is a security concern.

For an airport to obtain the certification required for operations, the airport operator must be able to maintain required airside operational clear areas and have adequate emergency response routes to allow first responders to meet appropriate response times.

4.1.2 Landside

Landside infrastructure is separate from terminal and airside facilities. In general, the landside facilities include 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.

Landside facilities provide both traveling passengers and the non-traveling public access to the terminal and airside of the airport. Since the landside includes all non-airside areas other than the terminal(s), its location is determined by the airside and perimeter boundary. Factors affecting the locations of facilities are discussed in Section 6, Landside.

As landside facilities do not directly affect the operation of aircraft, they generally have less stringent security requirements than the airside. However, some clear areas and communications requirements may still affect some landside design and layouts, such as an airside fence/boundary; aircraft approach glide slopes; communications and navigational equipment locations and non-interference areas; and heightened security in the terminal area. Further information on these requirements is contained in Security Areas.

In general, the landside must meet the local jurisdictional standards for public safety and security, which may result in special safety requirements that will interface with the airport's overall security and fire safety system.

4.1.3 Terminal

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

When considering passenger and baggage screening security provisions, it is important for planners and designers 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. Planners and designers are encouraged to discuss security considerations with the FSD and Fixed Base Operators (FBO) when developing charter or private aviation facilities, as well as when developing facilities intended for use by scheduled commercial air carriers or aircraft operators.

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 in close proximity to, the terminal. Since the terminal usually straddles the boundary between airside and landside, certain portions of a terminal must meet the requirements of both of these areas.

When designing a new facility, the terminal is typically centrally located on the airport site, when possible. 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-airport 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 Large Vehicle IED (LVIED) or Vehicle Borne IED 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.

4.2 Security Related Areas

Each Airport Security Program (ASP), developed under 49 CFR § 1542.101, contains descriptions of the following areas in which security measures are specified at each airport.

4.2.1 Air Operations Area

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 49 CFR § 1546, and any adjacent areas (such as general aviation and cargo areas) that are not separated by adequate security systems, measures, or procedures. This area does not include the Secured Area.

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 local 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 risk assessment or vulnerability assessment, 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. Refer to Boundaries for more information, and to Appendix A, Airport Vulnerability Assessment Process.

When allocating AOA space, planners should consider that the AOA requires fewer specific security measures than the higher requirements of SIDAs or Secured Areas. Therefore, maintenance or construction staging areas can have simpler access outside the more critical areas, and perhaps reduce the amount of personnel hours needed for issuing and revalidating ID media, performing background checks, and conducting security training.

4.2.2 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.

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

Although the Secured Area generally includes portions of the landside and terminal, it is desirable to locate Secured Areas contiguously or as close together as possible to maximize ease of access by response personnel, utilize common areas of CCTV surveillance coverage, and minimize requirements for redundant boundaries and electronic access controls. 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.

4.2.3 Security Identification Display Area

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. A SIDA may include other areas of the airport. Generally, the airport operator has the responsibility to secure SIDAs and prevent or respond immediately to access by unauthorized persons and vehicles. SIDAs may lie within AOAs.

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.

4.2.4 Sterile Area

A Sterile Area is a portion of an airport, specified in the ASP, that provides passengers access to boarding aircraft, and to which access generally is controlled by TSA, or by an aircraft operator under 49 CFR § 1544 or a foreign air carrier under 49 CFR § 1546, through the screening of persons and property.

TSA must use adequate facilities and procedures to screen persons and property prior to entry into the Sterile Area to prevent or deter the carriage of any explosive, incendiary, or deadly or dangerous weapon on or about each individual's person or accessible property. In addition, the aircraft operator must prevent or deter the carriage of any explosive or incendiary in any checked baggage brought into the Sterile Area.

Sterile Areas require physical, financial, and manpower resources dedicated to providing screening. Sterile Areas may include various revenue-generating concession facilities, which may be impacted by periods of heightened threat. Designers and planners should allow flexibility within Sterile Areas such that added security measures during times of heightened alert will have the least possible negative impact.

4.2.5 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.

Specific requirements and conditions must appear in the exclusive area agreement, which is then approved by TSA. Such conditions include a delineation of very specific 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.

4.2.6 Airport Tenant Security Program Area

An Airport Tenant Security Program (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.

Subject to a tenant area–specific security program approved by the TSA, the airport tenant assumes responsibility for specific security systems, measures, or procedures, except for law enforcement.

Where tenants other than air carriers elect to undertake under their own security programs under 49 CFR § 1542, 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.

4.3 Assessment of Vulnerable Areas

4.3.1 Concepts of Security Risk Management

Basic concepts of security risk management dictate that the security system provide the appropriate level of security for all of the assets to be protected, determined by an assessment of the perceived threat to those assets. At the facility planning stage, it is prudent to consider the relative “value” (or consequence of loss) and economic impact of all assets. There are many high value assets at an airport to consider, such as aircraft (with or without passengers aboard); air traffic support facilities (tower, radar, weather, and communications); terminal building(s), groups of the public or employees; fuel storage; critical infrastructure (power, water, and communications); and surface vehicle access and surrounding waterways/intermodal transportation facilities.

4.3.2 Fundamental Concepts for Airport Security

One of the fundamental concepts for airport security is the establishment of a boundary between the public areas and the areas controlled for security purposes (the described AOA, Secured Areas, SIDA, etc.) Since barriers and controls differentiate and limit access to these areas, this can lead to the assumption that anyone or anything found in the area is authorized to be there. This suggests a common vulnerability: once inside the controlled area, an intruder may move about with relative ease, without encountering additional controls. For example, if an intruder breaches the fence line, he may find no further physical barriers to control access to aircraft, the baggage makeup area, maintenance facilities, and other areas. Security measures often employed to mitigate this situation include challenge procedures augmented by ramp patrols, electronic monitoring (such as by CCTV), personnel surveillance, ground radar or intrusion detection sensors, and others, all of which have planning and design implications.

4.3.3 Unauthorized Access

Other means of achieving unauthorized access exist, such as through misuse of emergency exits from public side to the Secured Area, or passing through a controlled access portal opened by an authorized user, which is a practice often called piggybacking. New construction projects should minimize the number of emergency exits that lead to the Secured Area from public areas. Some fire codes allow the use of delayed egress hardware on emergency exit doors. Where authorized for use by fire or building code officials, delayed egress hardware should be considered for use as a deterrent to discourage unauthorized, non-emergency use of emergency exit doors. Where necessary, these doors can be supported by comprehensive CCTV surveillance on both sides of the door for alarm assessment. Ideally, the airside surveillance would include an intruder tracking capability to direct the response force.

Another point of concern is unauthorized entry or breach into the Sterile Area. Any open boundary between the public area and the Sterile Area is a candidate for such a breach. Typically, the breach will occur either through the passenger security screening checkpoint or via the exit lane (bypassing the security checkpoint).

4.3.4 Fundamental Vulnerability of Public Access Facilities

All public access facilities, within which large congregations of people are customary, suffer from a fundamental vulnerability to terrorist attacks. Considering blast mitigation at the planning and design stage can reduce this vulnerability significantly. For the threat of large vehicle bombs, the primary blast-mitigating consideration is separation distance. This consideration runs counter to the passenger convenience consideration of minimized transit distances. Innovative designs that satisfy both passenger convenience and separation distance for blast mitigation should be sought, including potential facility design to minimize large congregations of people close to points of vehicle access or drop-off, or blast resistant walls and barriers.

4.3.5 Vulnerability of Public Side within the Terminal

The threat of an armed attack on the terminal, or an abandoned article containing an explosive device, raises attention to another form of vulnerability. As long as there is a public side within the terminal, where concentrations of people are expected, there are limited means by which a security system can prevent an attack. Ensuring that LVIEDs, IEDs, or active shooters do not enter the terminal would require moving the point of screening to the front door. Architects and designers may seek to reduce this vulnerability through innovative designs that can balance passenger convenience issues with screening requirements.

4.3.6 Access Media/ID System Vulnerability

A potential vulnerability also exists in an access media/ID system that grants access privileges to employees and others. These “insiders” have legitimate needs for continuous access to the portions of the airport controlled for security purposes, and in some cases to the workings of the security system itself. However, threats from insiders, acting alone or in collusion with outsiders, can pose a criminal and terrorist threat to airports. The need to inspect individuals, their ID media, and their possessions as they cross the security boundary has increased in recent years, affecting the design of access gates and the procedures used to authorize access to the airside. At the planning and design stage, one goal should be to minimize the number of points that employees use to gain access to their work site. Infrastructure provisions for screening equipment at these locations would enable future inspection capability with significantly less impact. The same locations may also be considered as sites for inspection of deliveries of commercial goods, or for any future security requirements being mandated for employee access portals.

The FAA Extension, Safety, and Security Act of 2016[10], Section 3407 requires TSA to “develop a model and best practices” for random TSA “physical security inspections” of airport workers to verify credentials for SIDA access and screen for prohibited items not necessary for their duties. It also requires a TSA review of U.S. airports that have implemented “airport worker screening” at Secured Area access points, the perimeter, or elsewhere, and then “identify best practices” for dissemination to airport operators. Designers should plan for additional space allocations for screening equipment at employee points of entry for compliance with future TSA mandates.

4.3.7 Other Potential Areas of Vulnerability

There are numerous areas in and around an airport, its terminal building complex, support facilities, utility tunnels, storm sewers, construction entrances, public roadways, parking lots, maintenance areas, cargo and GA, commercial and industrial buildings, etc., which, while not necessarily recognized as the main target of terrorist activity, might still be in the path of such an attack. At the very least, these areas are often subjected to common crime (e.g., theft or vandalism), and may require varying levels of

[10] PL 114–190

security protection. These may or may not fall under the jurisdiction or responsibility of the airport operator, but it is important to look at the entire airport environment, make those determinations, and bring every affected entity into the early planning discussions, if for no other reason than to establish early on where the lines of responsibility lie. The airport operator must also keep careful records of these determinations and consider putting those agreements and lines of demarcation in writing, possibly as conditions of the lease, or into exclusive area or ATSP agreements.

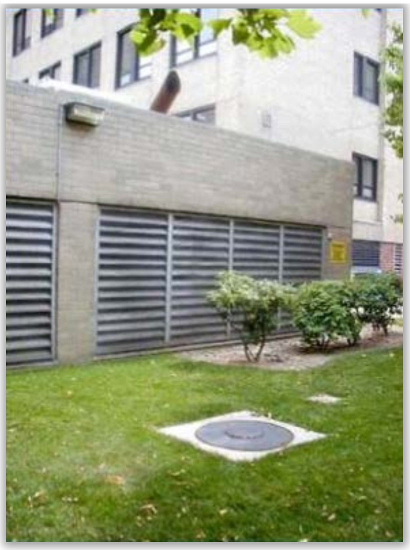
4.3.8 Utility Infrastructure

Utility sources, equipment, and supply potentially should be protected and/or monitored to the extent warranted by a threat and vulnerability assessment. Planners should contact the airport security coordinator and local FSD for any current studies relating to utility infrastructure security. The design of these systems should also reflect their importance for mission-critical operations of airports, with due consideration given to redundancy, backup systems, alternative sources, and the required levels of service, response times during emergency situations, and associated airport and non-airport organizational responsibilities.

In this context, *utilities* encompass electrical power, including both external services and on-airport generation and distribution systems; lighting; water and drainage systems; fuel farms including pipeline distribution and pumping stations; telecommunications (voice, video, data) including external wired and wireless services as well as on-airport networks and trunked radio systems used for public safety functions; and facility heating, ventilation and air conditioning (HVAC).

Electrical power is critical to an airport's operation. No major airport should be without alternatives to its primary electrical power supply, such as linkage to a second substation or, where feasible, a second regional grid, generated secondary power, and/or battery back-up or an Uninterrupted Power Supply (UPS) system with appropriate automated switching capability. Individual battery backup or UPS units to support access control systems during power outages are also highly desirable. Furthermore, the security design must provide distributed power for priority provisions (i.e., lighting, communications, etc.) HVAC systems have important functions during extreme weather conditions because they control and maintain ambient temperatures for equipment and thousands of passengers and employees.

Figure 4-1. Air Intake Vent



Source: FEMA

However, in doing so, HVAC equipment provides fresh air or heat circulation, which can become an attractive target or vector for attack. The security design should consider placing fresh air intakes in nonpublic areas whenever possible to control access to the intake vents. If it is not feasible to locate the air intakes in nonpublic areas, the security design should consider providing a capability to monitor publicly accessible air intakes (e.g., use of video cameras). Additionally, the security design should also provide for the capability to isolate sections of the building, and to vent sections of the building by using positive air pressure.

Tunnels and drainage provisions provide access into the building that may be exploited. Airport design should consider the security of the routes by which utilities enter and exit the terminal building, as well as culverts or storm sewers that cross under perimeter fences and roadways.

Fuel supplies for vehicle and aircraft operations require protection of the pipelines, fuel farms, or other facilities that are operationally sensitive and vulnerable to attack.

Water sources may merit protection, keeping in mind the function of the water for firefighting and human emergency support. Whether a water source is external or internal, the designer should assess the level of risk for all aspects of the system. The designer may consider protecting the water supply from interruption or the introduction of a contaminant; the designer should also consider the possibility of an alternative source.

Telecommunications services and the networks on which they run provide essential services for airport operations. Service entrance points for carrier services should be protected against both accidental and deliberate damage. Telecommunications rooms and operations centers are critical assets and should be secured by access control and CCTV systems. When network cabling traverses public areas, metal conduit should be used to protect the cabling.

In emergencies, having reliable, robust, and capable wireless communications for management, operations, and public safety functions will be essential. Public safety departments will often have their own trunked radio systems, which also support airport operations. Dependence on carrier cellular services should be minimized as these networks are often saturated by traffic during emergencies. A standards-based wireless extension of the airport local area network (LAN) can be valuable in emergencies, provided that operating frequencies and access point coverage have been properly designed and coordinated with all users, including tenants.

4.3.9 Seismic Requirements

Seismic requirements, while not innately a security issue, are relevant to security guidelines in that the continuity of airport operations is paramount to airport security.

This section provides references to various state and federal legislation addressing seismic safety. While much seismic engineering and mitigation guidance exists in the form of state and local codes, directives, and ordinances, these requirements focus only on acts that are currently in effect, not those being proposed for future planning and design needs.

The existence of these laws, codes, and directives does not necessarily indicate that they fully meet their intent, or that they necessarily accomplish their objectives. Some are considered more or less effective than others, and even some weaker ones may be enforced to a greater extent than others. Architects, engineers, and contractors should seek out expert opinion about the appropriateness and effectiveness of any specific seismic requirement as it affects their airport design.

It is important to note that all of the seismic laws and Executive Orders apply to virtually all new construction that is federally owned, leased, or regulated, or other new construction that receives federal financial assistance through loans, loan guarantees, grants, or federal mortgage insurance. Additionally, several states require seismic mitigation in the design of all projects.

When designing a project, it is important to meet the federal, state and local code and standard elements applicable to the project location. The following list is not comprehensive, but as an aid to the designer, it is recommended that the following sources of information be reviewed to determine any current requirements.

- Public Laws 95–124 and 101–614, "The Earthquake Hazards Reduction Act of 1977 as Amended."
- Executive Order 12699 of January 5, 1990, "Seismic Safety of Federal and Federally Assisted or Regulated New Building Construction."
- Executive Order 12941 of December 1, 1994, "Seismic Safety of Existing Federally Owned or Leased Buildings."
- ICBO (International Conference of Building Officials, "Uniform Building Code (UBC)," 1994, and amendments to include the 1994 National Fire Protection Association (NFPA) 13 Standard for Building Fire Sprinkler Systems.
- BOCA (Building Officials Code Authority (BOCA), "National Building Code."
- SBCCI (Southern Building Code Congress International "Standard Building Code."
- Section 13080 of the *Corps of Engineers Guide Specifications with Fire Sprinklers*, Sections 15330, 15331, and 15332 revised in March 1995 to unequivocally require seismic bracing on the small diameter piping.
- Various state building codes (e.g., California, Washington, Alaska, Missouri, New York, etc.), which may require mitigation elements in addition to the national standards.

4.4 Chemical and Biological Agents

When considering overall layout, it is prudent to take some precautions to prevent attacks against civil aviation by non-conventional means, such as the use of radiological, chemical, and biological agents. The possibilities for such attacks include the use of chemical or biological agents to attack persons in an aircraft in flight, as well as in public areas of airports, (see Section 7, Terminal) or persons in areas controlled for security purposes. Some measures that should be considered to help mitigate a potential chemical or biological attack include:

- Locate mailrooms and airport loading docks at the perimeter of the terminal, or at a remote location, with screening devices in place that can detect explosives and chemical and biological contaminants.
- If the mailroom and loading docks are in or near the terminal, consider having a dedicated ventilation system for those rooms, and dedicate an emergency shut-off device for the ventilation system.
- Take measures to seal off these areas from the rest of the terminal to minimize the potential for contaminants to migrate to other areas of the terminal. Maintain a slight negative air pressure in these rooms to help prevent the spread of the contaminants to other areas.
- Locate air intakes to HVAC systems so they are not accessible to the public. Preferably, locate air intake as high as practical on a wall or on the roof; if vents are at ground level, they should be protected if possible with screens or grates, and with openings facing away from public exposure.
- Coordinate the smoke control system and emergency power with the chemical/biological alarms and ventilation system.
- Consider installing special air filtration in critical ventilation systems that captures chemical and biological agents.

Additionally, at the direction of the DHS Science and Technology Directorate through the PROACT (Protective and Responsive Options for Airport Counterterrorism) program, the Sandia National Laboratories issued *Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism*, co-authored with the Lawrence Berkeley National Laboratories.

4.5 Boundaries and Access Points

To delineate and adequately protect the AOA, SIDA, and other security 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. However, when considering whether any natural barrier is an appropriate boundary, the airport operator should take into account the findings of the risk and vulnerability assessments prepared for the airport, and whether the natural barrier should be complemented with other types of boundary protection. Again, special attention should be given to areas where significant bodies of water are used as public recreational or fishing areas near the airport boundary. 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 to consider that would enhance these boundaries and access points are clear zones on both sides of fences, security lighting, locks, CCTV monitoring systems, and signage.

The choice 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. Certainly the highest consideration in an effective boundary measure is its ability to prevent unauthorized penetration. Thus, any access points through an intended portal of 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, more functional and maintainable access points that will benefit the airport in the long run.

Various boundary, barrier, and access point types, as well as security measures that can enhance them, are described below.

4.5.1 Physical Barriers

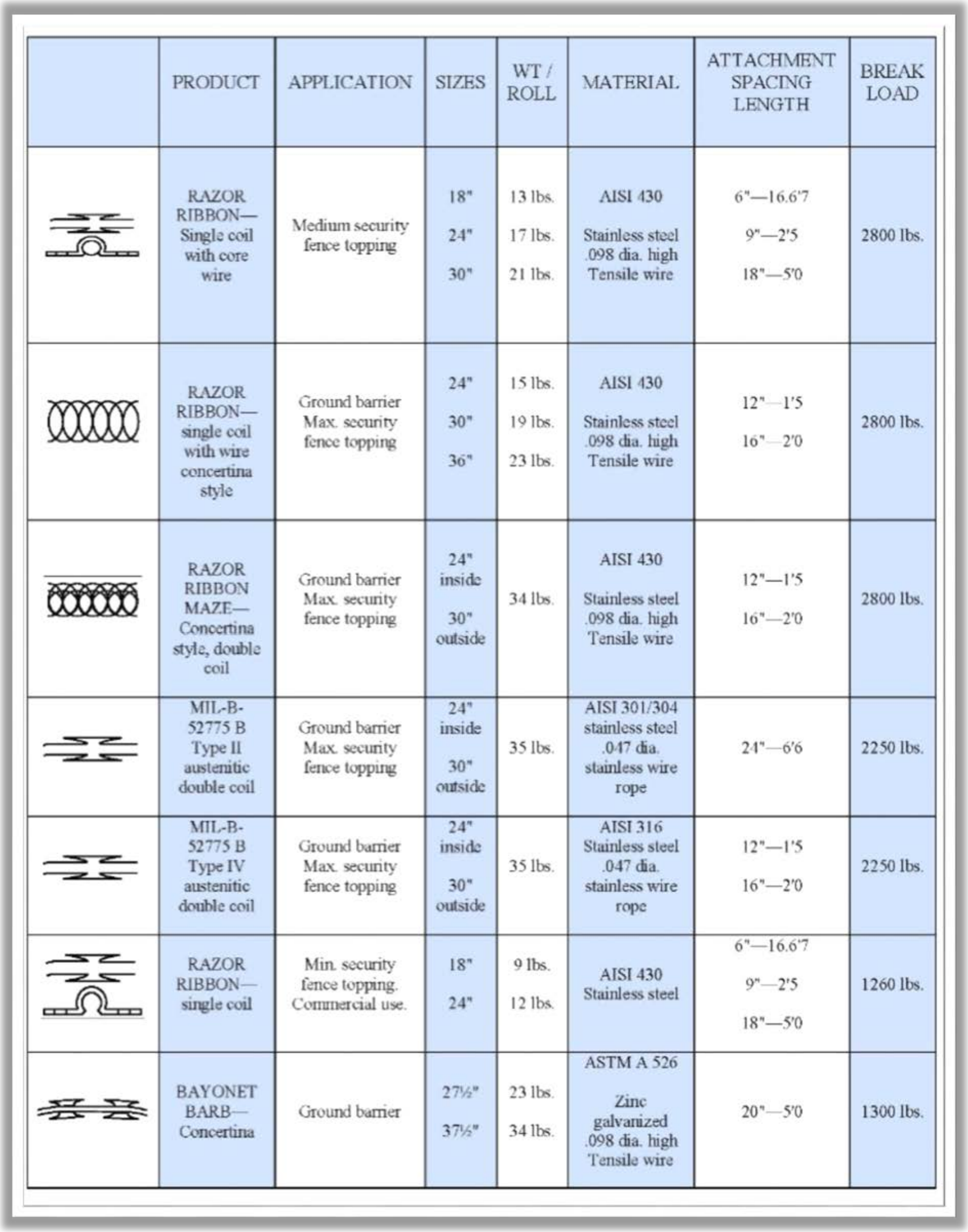
Physical barriers can be used to deter and delay the access of unauthorized persons into nonpublic areas of airports. These are usually permanent barriers and designed to be an obvious visual barrier as well as a physical one. They also serve to meet safety requirements in many cases. Where possible,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

4.5.1.1 Fencing

Some types of fencing are difficult to climb or cut, and many use such technologies as motion, tension, or other electronic sensing means. When fences have sensors, either mounted on the fencing or covering areas behind fencing, they must be accommodated in the security system to monitor the sensors and to initiate response to intrusion alarms. Table 4-1 shows some of the available types of fence fabrics with

American Iron and Steel Institute (AISI) and American Society for Testing and Materials (ASTM) ratings.

Table 4-1. Fence Fabrics and Construction



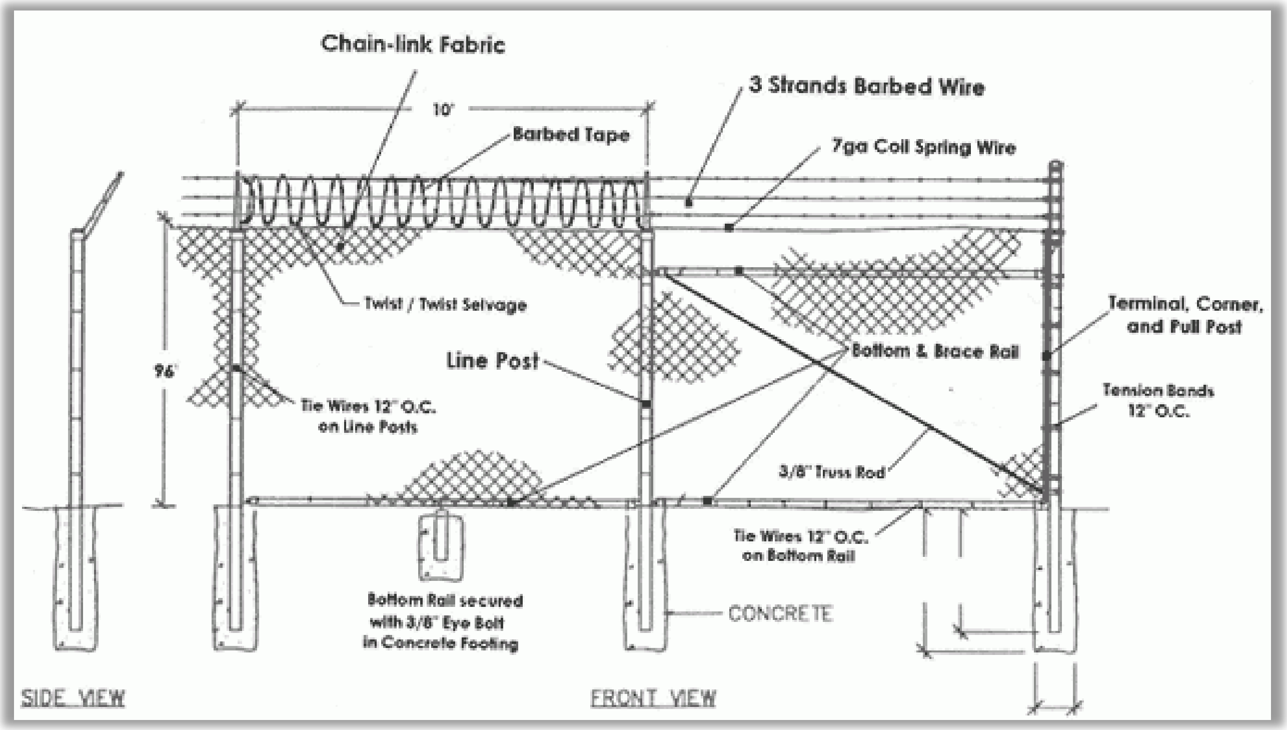
	PRODUCT	APPLICATION	SIZES	WT / ROLL	MATERIAL	ATTACHMENT SPACING LENGTH	BREAK LOAD
	RAZOR RIBBON—Single coil with core wire	Medium security fence topping	18" 24" 30"	13 lbs. 17 lbs. 21 lbs.	AISI 430 Stainless steel .098 dia. high Tensile wire	6"—16.6'7 9"—2'5 18"—5'0	2800 lbs.
	RAZOR RIBBON—single coil 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"—16.6'7 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 and cost-effective type of fencing for deterrence, as opposed to the prevention of forced entry. The FAA Advisory Circular recommends chain link fences to be constructed with seven feet of fabric plus one or more coils of stranded barbed wire on top, which may be angled outward at a 45-degree incline from the airside. Fabrics should be secured to the fence posts and to the bottom rail in a manner that makes it difficult to loosen the fabric (see Figure 4-2).

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.

Figure 4-2. Example of Chain Link Fencing Design



Source: Chain Link Fence Manufacturers Institute

For safety or operational reasons (e.g., presence of navigational systems), some sections of perimeter fencing may not be able to meet standard security specifications. Special surveillance or detection measures may need to be applied to improve the safeguarding of these areas.

4.5.1.2 Buildings

Buildings and other fixed structures may be used as a part of the physical barrier, and 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 perhaps 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 or maintenance access ladders do not provide an unobstructed path from the public side to airside.

4.5.1.3 Walls

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 separation. In addition, walls play an important part as visual barriers and deterrents.

Interior Walls
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 not just 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.

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

Walls of solid materials 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. Blast 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.

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 Secured Area is maintained to at least the level maintained elsewhere along the boundary.

4.5.2 Electronic Boundaries and New Technologies

Boundaries that are monitored by electronic sensors, motion detectors, and infrared or microwave sensors are intended to serve the same security functions as other detectors by employing alternative technologies. These technologies could have higher maintenance costs. They may be used in conjunction with other technologies such as alarms, CCTV, or other reporting and assessment methods. Nonetheless, there are appropriate places for using such applications, especially where normal conduit and cabling might be impractical, or where excessive trenching might be required. In addition, new technologies that involve existing FAA ground radar surveillance can be incorporated for use in a security mode.

While this document is focused on initial planning and design for current projects, new facilities such as terminals may sometimes take four or five years from the drawing board to processing the first aircraft and its passengers. When planning that future terminal, and all other related facilities requiring a security perspective, designers must also take into account continuing developments throughout the airport industry and the technologies that contribute to its secure well-being. While it may not be possible or even prudent to adopt first-generation beta-version technologies (although there may also be some corresponding advantages in such an approach), it is virtually certain that technology developments in many areas will afford new security capabilities and new requirements in the foreseeable future. The lesson learned is that the airport operator must stay alert to new technologies and trends, and the early design should remain flexible to accommodate any such developments where appropriate.

4.5.3 Aircraft Maintenance Facilities

Aircraft maintenance facilities may be located completely landside, completely airside, or part of the airside/landside boundary line. As these facilities contain protected areas and also involve 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/opening as a security boundary/demarcation line
- Location of loading/delivery docks landside

4.5.4 Aircraft Movement Areas

By definition, aircraft movement areas (runways, taxiways, and aircraft ramps) 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.

4.5.5 Aircraft Rescue and Fire Fighting Facilities

ARFF stations and equipment are a requirement of 14 CFR § 139, Subpart D, Certification and Operations: Land Airports Serving Certain Air Carriers, which is administered by the FAA. These facilities are clearly critical to an airport’s operations. Even in a multi-station environment, the primary ARFF station may be located straddling the airside and landside boundary. This positioning may be necessary for a variety of reasons, but public access to the ARFF station may be needed as well as for mutual aid responders and for ease of landside access to the ARFF station for the fire fighters themselves. However, public access in a multi-station scenario 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 airport tenant employees 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, other portions of the ARFF station must be controlled to prevent unauthorized access to the airside.

4.5.6 Security Operations Center and Airport Emergency Command Post

Typical titles for facilities where normal security dispatch and operations occur include Security Operations Center (SOC) and Airport Operations Center. Typical titles for facilities where airport emergency operations occur include Airport Emergency Command Post (CP) and Airport Emergency Operations Center. A distinction is made between non-emergency (everyday operations) and emergency facilities, which are established for command and control operations during emergencies.

Demand for SOC and CP facilities may be for a single event or potentially, multiple events happening concurrently. It may also be necessary to provide redundant SOC and/or CP systems within alternate facilities at another airport area.

There are no hard and fast rules for these locations, though most are in or attached to the main terminal. In all cases, they should be located within a Secured Area. The designer should discuss alternative proposed locations with all departments who will use the SOC and/or CP. Indeed, secondary or satellite locations may be valuable for those instances when the primary SOC or CP is out of service, or when multiple events are taking place. While ease of access to the airside is one primary consideration, there are numerous other concerns, such as sufficient operating space for police and other support personnel, central location for access or dispatch to any point on the airport, technical considerations such as cable routing for all necessary equipment, or support services such as restroom or break room amenities. Considerations for public accessibility should also be considered for SOC facilities based on procedures for public-related systems and services such as paging, lost and found, or first aid.

For a discussion of these areas and their contents, see Section 15, Command and Control.

4.5.7 Airport Personnel Offices

Most personnel and administrative offices have landside and/or public access during business hours. During non-business hours, they are usually secured, and may be included in the airport’s overall access control system, particularly if located within the terminal complex. Most airport personnel offices are located in or near the terminal, and are secured (nonpublic) at least part of the time. Some airport offices, such as airfield maintenance or operations, are generally completely airside, but still behind access controls.

4.5.8 Belly Cargo Facility

Belly cargo is that which is carried on passenger aircraft rather than all-cargo or freighter aircraft. Belly cargo facilities share most of the same security requirements as standard cargo areas, and in many airports may be part of a single joint cargo facility or area. A facility for shared cargo screening, including belly cargo and regular cargo, certainly should be considered.

However, some airports maintain a completely separate area for belly cargo. Since most belly cargo is delivered via tugs, a belly cargo facility can be located either adjacent to the terminal where the aircraft are, or at any point along a service roadway that connects to the terminal. In that event, it is important that the tug route be considered for potential congestion and/or blind spots.

The added flexibility in the location of a belly cargo facility, as well as the fact that it can be separate from the general cargo facility, enables it to be designed with potentially higher security levels. Since belly cargo usually involves smaller quantities of public air cargo and U.S. mail, belly cargo facilities can be designed that have the potential for 100 percent Explosives Detection System screening of cargo, and have more flexibility than direct cargo-to-plane operations in that the facility can be either landside or airside, and still be isolated from critical passenger aircraft areas.

4.5.9 All-Cargo Area

A general all-cargo area includes all the ground space and facilities provided for cargo handling. It also includes airport ramps, cargo buildings and warehouses, parking lots, and associated roadways.

4.5.10 FAA Airport Traffic Control Tower and Offices

The FAA Airport Traffic Control Tower (ATCT) and its administrative offices may be located within or adjacent to a terminal complex or in an airside or landside area. ATCT location is dependent upon runway configuration and line-of-sight criteria. ATCT security needs should be coordinated by the airport planner and designer such that an interface takes place with FAA security requirements pursuant to FAA's ATCT design criteria. 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 upon airport operations.

4.5.11 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, and should be access-controlled whenever possible to monitor all movements, including authorized traffic. Where distance precludes hard wiring to the main system, there are wireless technologies as well as freestanding electronic locking mechanisms available. CCTV monitoring, alarms, and sensing should be considered in and around fuel farms and storage tanks to alert law enforcement and security personnel of potential intruders or tampering.

4.5.12 General Aviation and Fixed Base Operator Area

GA and FBO areas at commercial passenger airports are airport tenant areas that typically consist of aircraft parking areas, aircraft storage and maintenance hangars, and/or tenant terminal facilities. GA and FBO areas are usually part of the airside/landside boundary; aircraft parking areas/ramps are located airside.

Information on security at non-commercial GA airports is found in Appendix D. TSA Information Publication (IP) A-001, *Security Guidelines for General Aviation Airports*, issued in May 2004 is also available on some aviation web sites.[11]

This material should be considered a living document that will be updated and modified as new security enhancements are developed, and as input from the industry and other interested parties is received.

4.5.13 Ground Service Equipment Maintenance Facility

Most airports maintain specialized areas for storage and maintenance of ground service equipment (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

[11] As of the date of this document, a complete update is underway, and is expected to be available in calendar year 2017.

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 and vehicle parking and storage areas, ensuring they do not compromise airside fencing clear zones or security.

4.5.14 Ground Transportation Staging Area

A Ground Transportation Staging Area (GTSA) is a designated area where taxis, limos, buses and other ground transportation vehicles are staged prior to reaching the terminal curbside areas. These areas are always landside as they involve public and private off-airport transportation services.

4.5.15 Hotels and On-Airport Accommodations

Hotels and similar on-airport public accommodations are normally landside, although in some configurations may overlook airside, or have direct lines-of-sight to the AOA/SIDA. Refer to Section 6.5.2, Hotel and On-Airport Accommodations.

4.5.16 Industrial/Technology Parks

Industrial/technology parks may be landside, airside or have elements of both. Many airports have land available or in use as industrial/technology parks. Planners should evaluate this land use for security impacts to the airport’s operations, particularly along shared boundaries.

4.5.17 In-flight Catering Facility

On-airport facilities for in-flight catering service may be located landside, airside, or may be a boundary facility with portions of both. Due to the nature of the facility, as well as its typical placement near the passenger terminal, security requirements may involve substantial amounts of coordination, both architecturally and procedurally. The results of the security risk and vulnerability assessments involving catering operations should be evaluated in advance of design or construction of these facilities.

4.5.18 Intermodal Transportation Area

The function of an intermodal transportation area is to transfer passengers or cargo from one mode of transportation to another. While intermodal transportation areas vary greatly in function and location, they are typically always completely landside facilities, although they may border or overlook airside, particularly when raised above ground level. Detailed information is in Section 6.5.3, Intermodal Transportation Areas.

4.5.19 Isolated Security Aircraft Parking Position

The Isolated Security Aircraft Parking Position is a location within the airside, and is used for parking an aircraft when isolation is required due to security or other concerns. This location is subject to special security requirements as identified in the airport’s ASP or Airport Emergency Plan (AEP).

Detailed information is contained in Section 5.1.5, Isolated Security Aircraft Parking Position.

4.5.20 Military Facilities

Some airports may have adjacent or on-airport military facilities, such as Reserve, National Guard, State, U.S. or active duty units. Since each of these situations is unique, and since these facilities may be partially airside, detailed coordination between the airport operator, FAA, TSA, and the government military facility should occur to consider both design and procedural accommodations. Typical areas of coordination include access control, ID systems and background check requirements, areas of access, security patrol boundaries, blast protection, security response responsibilities, and joint and/or shared security system data and equipment. Proper coordination should also occur to ensure that the security and safety of such military facilities are not compromised by the placement of airport CCTV and access control equipment. See *Unified Facilities Criteria UFC 4-010-02 for Department of Defense (DOD) Minimum Anti-Terrorism Standards* for buildings used by the military.

4.5.21 Navigational and Communications Equipment

Since the placement of navigational and communications equipment is typically driven by functionality, not security, most airports have equipment both airside and landside. Where equipment cannot be airside, it should be fenced for both safety and security. In addition, electronic monitoring and/or controlling of access to critical equipment is desirable.

4.5.22 Passenger Aircraft Loading/Unloading Parking Areas

Passenger aircraft loading/unloading equipment parking areas are required to be airside, are typically at or near the passenger terminal within the Secured Area, and require security measures.

4.5.23 Passenger Aircraft Overnight Parking Areas

Passenger aircraft overnight parking areas are required to be airside and are usually adjacent to the passenger terminal, but may also be on a designated remote ramp. These areas are required to be within the AOA or Secured Area, and require security measures per 49 CFR § 1544.

Additional information is contained in Section 5.1.3, Passenger Aircraft Overnight Parking Areas.

4.5.24 Rental Car and Vehicle Storage Facilities

Rental car facilities and vehicle storage are usually landside, often well removed from the terminal, and may or may not be part of the airport's security responsibilities.

See Section 6.5.4, Rental Car Storage Areas.

4.5.25 State/Government Aircraft Facilities

Some airports include areas for non-military government aircraft support facilities. For the most part, these facilities should be given the same considerations as GA/FBO areas. However, because of their nature, non-military government aircraft support facilities are often isolated from other GA/FBO areas, and require stricter, and more extensive, security measures. In many cases, these areas will have their own, independent security/access control/CCTV system, as well as their own monitoring and security personnel; however, procedural coordination and communication with the airport should still occur.

4.5.26 Terminal Patron Parking Areas

Terminal patron parking areas are public areas and are required to be completely landside. Parking areas are typically at or near the passenger terminal, but may also be located remotely. Security requirements for patron parking areas varies greatly, and is dependent upon the area's proximity to the passenger terminal, security areas, and perimeter fencing, and methods used to control entry to the parking areas.

4.5.27 Utilities and Related Equipment

Design and location of utilities and related equipment and service areas should be coordinated with security and fencing design to minimize security risks and vandalism potential. While it is beneficial from a safety and vandalism standpoint to locate utility equipment airside when possible, maintenance contracts and service personnel ID media issuance and access may require utilities or access points to be landside. Special emphasis should be given to above-ground electrical substations.

4.5.28 Through-the-Fence Agreement

Commercial and GA airports may have a Through-the-Fence Agreement authorized on a case-by-case basis by FAA, by which a landside entity that owns an aircraft on land contiguous to the airport would pursue an agreement with the airport operator to allow the aircraft to have access to the airport's taxiways and runways. The FAA is the approving authority; the landside entity is required to provide security and adherence to 14 CFR § 139 to the satisfaction of the airport and the FAA.

Where underground service ducts, storm drains, sewers, tunnels, air ducts, trash chutes, drainage structures, and other openings provide access to the airside or other restricted areas, security treatments such as bars, grates, padlocks, or other effective means may be required to meet practical maximum opening size requirements. For structures or openings that involve water flow, consider in the security treatment design the direction of flow, type and size of potential debris, and frequency and method of maintenance access required for debris removal, as well as the potential for flood and/or erosion during heavy flow/debris periods.

4.6 Checklists

Airport Layout and Boundaries Checklist

□ Determine general security requirements based on ConOps

□ Security & Safety Considerations
  - Separate dangerous or hazardous areas
  - Minimize concealed/overgrown areas
  - Effects on/by adjacent facilities
  - Natural features that might allow access
  - Communications interference from buildings & equipment
  - Public safety and security concerns
  - Criminal activity

□ Airside
  - Maintain airside/landside boundaries
  - Maintain clear areas and zones
  - Adequate emergency response routes
  - Required clearances

□ Landside
  - Public safety & security
  - Maintain airside/landside boundaries
  - Maintain security clear zones
  - Deter criminal activity

□ Terminal
  - Maintain public/nonpublic boundaries
  - Maintain security area boundaries
  - Meet security regulations
  - Personnel security and safety
  - Public security and safety

Security Areas Checklist

□ AOA
  - Perimeter generally defined by fences or natural boundaries

□ SIDA
  - May be a separately designated area located on AOA
  - Not necessarily a Secured Area (access controls not required)
  - Smallest manageable contiguous size(s)

□ Secured Area
  - Always a SIDA
  - Consider general aviation, cargo, maintenance, and other facilities in a manner consistent with TSA regulation and policy guidance

□ Sterile Area
  - Minimize size to help surveillance and control

□ Exclusive Use Area
  - Minimize areas to be monitored/controlled

□ ATSP Areas
  - Minimize areas to be monitored/controlled

Vulnerable Areas Checklist

□ Vulnerability Assessment (see Appendix A)

□ Consider all assets, targets, and their relative value/loss consequence
  - Aircraft
  - Communications
  - Support facilities
  - Terminal
  - Public and employees
  - Fuel areas
  - Utilities
  - Roadways and access ways
  - Storage areas

□ Establish a security boundary between public and Secured Areas
  - Barriers
  - Patrols
  - Surveillance/CCTV

  - ▪ Sensors

□ Minimize means of unauthorized access
  - ▪ Access controls
  - ▪ Emergency exits
  - ▪ Delay hardware
  - ▪ Piggybacking

□ Surveillance/CCTV

□ Plan for breach control measures and procedures
  - ▪ Physical barriers
  - ▪ Separation distance

□ Reduce bombing/armed attack vulnerability
  - ▪ Blast Mitigation
  - ▪ Separation distance
  - ▪ Minimize large congregations
  - ▪ Placement of screening checkpoint

□ Minimize vulnerability from employees
  - ▪ Minimize numbers of employee access points
  - ▪ Capability for employee screening

□ Consider vulnerability of adjacent areas and paths of travel

Chemical and Biological Agent Checklist

□ Sources of guidance may include TSA, FEMA, FBI, Department of Energy (DOE), CDC, and Office for Domestic Preparedness Support

□ References in bibliography list several relevant chem-bio documents.

□ Other Security Measures
  - ▪ Clear zones, security lighting
  - ▪ Consider life cycle costs and labor requirements, not just initial capital cost
  - ▪ CCTV Coverage
  - ▪ TSA/FAA-required signage per A/C 150/5360-12C
  - ▪ Instructional/ legal signage; coordinate with airport policy

Facilities, Areas and Geographical Placement Checklist

□ Facility Placement Considerations
  - ▪ Interaction among areas
  - ▪ Types of activity in each area
  - ▪ Flow of persons to/through areas
  - ▪ Delivery and maintenance traffic
  - ▪ Need for security escorts

□ Each Airport is unique

□ Facilities
  - ▪ Aircraft maintenance facilities
  - ▪ Aircraft overnight parking area
  - ▪ ARFF facilities
  - ▪ SOC/CP
  - ▪ Airport personnel offices

- Belly cargo facility
- Cargo area
- FAA ATCT and offices
- Fuel area
- GA areas
- GSEM facility
- GTSA
- Hotels and other accommodations
- Industrial/technology parks
- In-flight catering facility
- Intermodal transportation area
- Military facilities
- Navigation/communications equipment
- Rental car facilities
- State/government aircraft facilities
- Utilities and related equipment

SECTION 5: AIRSIDE

5.1 Aircraft Movement & Parking Areas (14 CFR § 139)

While the location of aircraft movement and parking areas is most often dictated by topography and operational considerations, the placement of the airside/landside boundary and the respective security boundaries should be carefully considered. The most important of these considerations is the placement of security fencing or other barriers. The following sections discuss security concerns for both normal aircraft movement and parking areas, as well as the aircraft isolated/security parking position.

5.1.1 Aircraft Movement Areas

Normal aircraft movement areas include all runways, taxiways, ramps, and/or aprons. While no specific security requirements state how far within the airside/landside security boundary these items must be, there are other operational requirements that that will affect security design and should be considered.

First and foremost among the non-security requirements are the FAA safety and approach runway protection zone requirements, as described in 14 CFR § 77. While the specific distance requirements vary by runway, taxiway, and/or aircraft class and wingspan, they all share the same types of requirements noted below. Although these are not security related areas, their location, orientation, and boundaries may have security implications (e.g., fencing, communications/interference, lighting, sight lines, etc.) FAA protection zones may include Object Free Area, Building Restriction Lines, Runway Protection Zone, Runway Safety Area, Glide Slope Critical Area, Localizer Critical Area, and Approach Lighting System. See FAA A/C 150/5300-13.

5.1.2 Passenger Loading/Unloading Aircraft Parking Areas

Security planning recommendations for parking passenger aircraft for loading and unloading at or near the terminal, including aircraft parked at loading bridges, should include consideration of the distance to fence/public access areas; distance to other parked aircraft awaiting loading, unloading, or maintenance; minimum distance recommendations for prevention of vandalism and thrown objects, etc.; and visibility of the areas around the parked aircraft to monitor for unauthorized activity. Typically, the passenger loading/unloading area is included as part of the airport’s Secured Area, which is also a SIDA.

5.1.3 Passenger Aircraft Overnight Parking Areas

Passenger aircraft overnight parking areas are generally not far removed from the arrival and departure gates. Where an aircraft must be moved for operational reasons to a parking area other than the airline’s maintenance or service facility, the design of its security environment should receive the same attention as the maintenance parking area, since its status as a passenger carrying aircraft has not changed, only the time spent in waiting. Where such overnight parking areas are relatively remote, they should be monitored and be well lighted, with no visual obstructions.

5.1.4 General Aviation Operations and Aircraft Parking Area

It is advisable, to the extent possible, to exclude separate general aviation (GA) areas from the SIDA of the airport. However, this is not always possible, as in the case where international GA flights, which would include charters, private, and corporate flights, must be directed to an International Arrivals Building area. Some unique considerations may be required where, for example, GA at smaller airports may operate from the same terminal as commercial aviation, sometimes found within or attached to the Secured Area at the main terminal.

Taxiways leading to the GA areas should, if possible, be planned to avoid ramps used by scheduled commercial passenger aircraft airline operations.

GA tenants should always be a part of the planning process for security-related matters that may affect their operations, and their staff should be appropriately badged for airside access.

5.1.5 Isolated/Security Parking Position

The International Civil Aviation Organization (ICAO) Standards require the designation of an isolated security aircraft parking position suitable for parking aircraft known or believed to be the subject of unlawful interference; to examine cargo, mail, and stores removed from an aircraft during bomb threat conditions; or which for other reasons need isolation from normal airport activities. This location is also referred to as a “Hijack/Bomb Threat Aircraft Location” or colloquially as the “hot spot” in many Airport Security Programs (ASP). Planners and designers are urged to gather input on ideal locations for these positions from those security or law enforcement agencies that will respond to such incidents.[12]

The isolated parking position should be located at the maximum distance possible (ICAO Annex 14 advises the allowance of at least 328 feet or 100 m) from other aircraft parking positions, buildings, or public areas and the airport fence. If taxiways and runways pass within this limit, they may have to be closed for normal operations when a threatened aircraft is in the area.

The isolated parking position should not be located above underground utilities such as gasoline tanks, aviation fuel storage tanks and pipelines, water mains, or electrical or communications cables or ducts.

Isolated aircraft parking areas would ideally be located to eliminate the possibility of unauthorized access to or attack on aircraft. Consideration should be given to the parking area’s visibility to and from public and press areas. Areas visible from major roadways should also be avoided to prevent roadway obstructions and accidents due to onlookers.

Availability of surveillance equipment, such as CCTV, to view the suspect aircraft and surrounding area may be beneficial to emergency response and/or negotiations personnel. Surveillance might come from repositioned perimeter cameras or video-equipped mobile command post communications support.

Consideration should be given to adjacent areas in which emergency response agencies (both personnel and vehicles) can enter and be staged during the incident. Communications; utilities and facilities; victim isolation, treatment and/or interview areas; and other features may be accommodated based on the respective airport’s Emergency Plan as required under 14 CFR § 139 and coordination with local agencies. Availability of CCTV surveillance coverage to view the suspect aircraft and surrounding area may be beneficial to emergency response and/or negotiations personnel. The area’s capability for cellular, radio, and other wired or wireless methods of communication should also be considered.

[12] Additional guidance in ICAO Annex 14 (Aerodromes), Annex 17 (Safeguarding International Civil Aviation Against Acts of Unlawful Interference), and ICAO Doc 8973 (Security Manual).

5.2 Airside Roads

Roadways located on the airside should be for the exclusive use of authorized persons and vehicles. Placement and number of airside roads should not only consider standard operational and maintenance needs, but also emergency response access to crash sites and isolation areas as itemized in the Emergency Plan. Perimeter roads should be airside, and should provide a clear view of fencing. Airside roads are intended principally for the use of maintenance personnel, emergency personnel, and security patrols (an ICAO recommendation). Where landside roads must be adjacent to airport fencing, a clear zone adjacent to fence should be established.

5.3 Airside Vulnerable Areas and Protection

The airport designer, in concert with security and operations leadership, should consider such things as NAVAIDS, runway lighting and communications equipment, fueling facilities, and the FAA's own air traffic facilities when developing an overall integrated security plan, as well as meeting the specific and unique security requirements for each such area. There is no single plan template that appropriately or adequately covers all these issues; it becomes the job of the architect, space planner, and designer to meet with all interested parties to suggest a balance among all these concerns. Protection includes not only from physical breach or damage, but also from both intentional and accidental electronic interference.

5.4 Airside Cargo

To the extent possible, air cargo facilities should be significantly separated from critical passenger loading areas and GA areas, and the ramp area adjacent to their air cargo facilities should be designated as a SIDA. Taxiways leading to the cargo areas, if possible, should be planned to avoid ramps used by commercial passenger aircraft operators.

5.5 Checklist

Airside Checklist

- □ To support aircraft operations, ramp areas should be securable
- □ Factors influencing boundary locations:
  - ▪ Aircraft Movement Areas
    - ▸ Runways, taxiways, ramps (See A/C 150/5300-13)
    - ▸ FAA safety and operational areas
      - Object Free Area
      - Building Restriction Lines
      - Runway Protection Zone
      - Runway Safety Area
      - Glide Slope/Localizer Area
      - Approach Lighting System
  - ▪ Passenger Aircraft Parking Areas
    - ▸ Safe distance to fence
    - ▸ Safe distance to aircraft
    - ▸ Distance—prevent vandalism
    - ▸ Monitor parked aircraft areas
  - ▪ General Aviation (GA) Operations/ Parking Area

    - GA not in Secured Area
    - Distance GA from terminal
    - Coordinate with tenants
  - Isolated/Security Parking Position (See ICAO Standards Annex 14 & 17
    - At least 100 meters clearance
    - Separate from utilities/ fuel
    - CCTV view -aircraft and area
    - Emergency staging area
    - Avoid public viewing/ areas

- □ Airside Roads
  - Restrict access to authorized vehicles
  - Perimeter roads should be airside
  - Perimeter roads - have views of the fence
  - Positioning of roads should consider:
    - Patrols
    - Maintenance Access
    - Emergency Access and Routes
  - Maintain fencing clear area

- □ Airside Vulnerable Areas
  - NAVAIDS
  - Runway lighting
  - Communications equipment
  - Fueling facilities
  - FAA ATC

SECTION 6: LANDSIDE

The landside is the area of an airport, including buildings and other structures, to which both traveling passengers and the non-traveling public have unrestricted access. Examples of landside facilities are public and employee parking, terminal and public roadways, rental car and ground transportation operations, hotel facilities, and commercial and industrial developments. Although the publicly accessible areas of terminal buildings are technically considered part of landside, terminals have a number of security-related considerations that are addressed elsewhere in this document.

Security in landside areas is difficult to monitor and control due to public accessibility and the limitations of implementing security measures—often over varied terrain, or in some cases urban settings immediately adjacent to airport properties. There are many issues to address while keeping focused on terminal design, passenger throughput, and the generation of revenues from sources ranging from retail operations to golf courses.

When considering TSA requirements for airport security, all landside area operations might be considered vulnerable targets; yet, basic tenets of physical security remain applicable. Improved technologies and prudent use of CCTV should be considered for airport security in coordination with airport law enforcement, airport operations, and the cooperation of tenants.

6.1 Natural Barriers

The use of natural barriers in the airport landside area may be advantageous in locations 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. As is the case in the airport airside area, with TSA approval, natural barriers may be incorporated into the security boundary of an airport in support of standard physical barriers, or as a complement to additional security measures or procedures.

Refer to Natural Barriers in the Layout and Boundaries section of this document for a description of possible natural barriers.

6.2 Landside Roads

When planning landside roadways, attention should be given to adjacent security fencing, airside access, and potential threats to terminal or aircraft operations. Should security levels be elevated, planners should consider the method and location for performing cargo and other vehicle inspections. This may involve electric utility installations, site preparation, and security IT data and communications lines.

Designers should bear in mind landside road proximity to security fencing, the potential for unauthorized airside access offered by elevated roadways, and line-of-sight threats to adjacent areas of the terminal, apron, and/or nearby aircraft. When an alert is issued, designers should consider potential methods and locations for performing vehicle inspections outside of the “blast envelope” established in the Blast Analysis Plan (BAP) for the terminal (see Appendix B). This can be accomplished with temporary or permanent inspection stations positioned on the approach roads. Vehicle inspection stations should include conduit and rough-ins at those locations for power, communications, and security data lines. If physically possible, consideration should be given to the creation of a roadway system that separates cargo from passenger vehicle traffic.

6.2.1 Vehicle Inspection Stations

Staffed vehicle inspection stations to control access in and around the airport terminal during elevated threat levels are advisable. These can provide locations outside of the blast envelope at which to inspect vehicles approaching the airport terminal on the access roadways. In some instances, vehicle inspection stations are also suggested at vehicle parking locations if they are positioned within or adjacent to the blast envelope.

Consideration should be given to including the following features at vehicle inspection stations:

- Turnstiles, roll gates, or vehicle crash barriers that will stop or impede “gate crashing.”
- A sheltered checkpoint station to permit maximum visibility over the immediate area of the gate, and to provide easy access for inspections. A sheltered checkpoint station could be a portable plug-in unit if utilities have been pre-positioned.
- Sufficient space to direct a person or vehicle to one side for further inspection without blocking access for those following. Also, sufficient space for emergency vehicles and other preauthorized vehicles to bypass the vehicle inspection stations.
- Provide communications, including emergency and duress alarms, between any sheltered security checkpoint station and the airport security services office.
- Ample vehicle queuing distance and inspection portals to avoid long traffic backups and delays during peak use times.

6.2.2 Roadway Design

Roads to the terminal should allow for uncongested flow during peak hours so as to ensure that law enforcement officers (LEO) have the ability to effectively monitor and move vehicles. Lines of sight for CCTV surveillance are a consideration, which may also serve to reduce the need for LEO response.

Drop-off and loading zones should be set as far away from the terminal as practical to minimize the blast effects of a vehicle bomb. Planners should consider the use of moving sidewalks or access to luggage carts to help passengers bridge the gap.

Planners should provide for emergency vehicle (fire and police) parking and staging areas near the terminal, potential inspection areas, and congested areas.

During periods of heightened security, planners should ensure vehicles cannot gain access to the terminal by bypassing the inspection area; aspects such as the potential to jump curbs, travel across open landscaping, or drive the wrong way down a road should be evaluated.

Planners can minimize traffic to the terminal by offering alternative routes to non-terminal based operations, such as access to the air cargo operations area, rental car agencies, hotels, or remote parking with shuttle service.

The airport should provide clear signage and allow for sufficient traffic lanes to permit drivers to find destinations easily. During periods of heightened security, airport operators should allow exit points or alternate routes prior to security checkpoints so that drivers may choose other options to access the terminal (such as buses or walking). This will help alleviate some congestion and inspection requirements. Roadways to and from cargo facilities should have geometry and turning radii sufficient to accommodate tractor-trailer traffic.

6.3 Landside Parking

During high threat periods, special security measures identified in an airport's BAP often prohibit the parking of unauthorized, un-inspected vehicles close to, beneath, or on top of the terminal, to minimize effects from a vehicle bomb. Planners should consider allowing temporary parking or inspections at a safe distance outside of the established blast envelope between parking lots and access roadways to the terminal.

Parking area entrances and exits should not be placed directly in front of the terminal. Elevated security levels may require inspections of vehicles entering and exiting, as well as stationary (already parked) in case of a shifting threat level.

Some underground parking facilities and rooftop parking areas in close proximity to the terminal or other critical infrastructure may also be subjected to special security measures during a high threat period. Designs should accommodate permitting vehicle access only after a detailed inspection process, closing parking areas off, or segmenting them in order to control access only by authorized personnel such as employees, first responders, or other known entities.

- Parking areas can be sectioned by a variety of mechanical devices. A common method involves the use of "head knockers"—immobile steel bars that suspend from the ceiling to limit the size of vehicles entering the area; the bars hang at the limiting level to stop large vehicles but allow smaller vehicles to proceed unhindered.

  NOTE: Emergency responders must be made aware of these limitations, and appropriate access points must be established for their needs, not just at the entrance, but at all ramps up and down the multi-level parking structure, which may include a very tight turning radius on circular ramps.

- Restricted parking areas should not be accessible by curb jumping or entry through the exit lanes. Fencing, bollards, or landscaping can often limit how close a vehicle can get, but will not provide blast protection.

Planners should provide sufficient space in parking areas to facilitate the movement of police, fire, and emergency vehicles, as well as turning radius accommodations for tow trucks for removal of suspicious or abandoned vehicles.

General security of parking and toll areas includes the need to consider cash-handling operations, and the potential for criminal activity such as robbery, assault, or auto theft. CCTV, lighting, intercoms, and duress buttons may need to be integrated with the main airport security system.

6.4 Employee Parking

Protection of employee parking areas, and the employees who use them 24 hours a day, is no less important than that of parking areas for the traveling public, and should be treated similarly, especially where they are remotely located and/or vulnerable to vandalism. Employee parking areas may be designed to include the same access control system used throughout the airport. Different parking lots can be considered as separate zones, keeping unauthorized use to a minimum. Space should also be allocated for employee screening checkpoints as appropriate. For cargo facilities, there should be no employee parking adjacent to cargo bay doors.

6.5 Landside Facilities

6.5.1 Ground Transportation Staging Area

Ground Transportation Staging Areas (GTSA) may present some unique security and safety concerns, and should be addressed in the planning and design phases. The U.S. DOT has developed security design guidelines for rail, bus, and other types of ground transportation systems, which parallel the contents of this Design Guidelines document. The DOT document *Transit Security Design Considerations* published by the John A. Volpe National Transportation Systems Center contains useful information for airport planners and designers.

6.5.2 Hotels and On-Airport Accommodations

Airport hotels are often found within or attached to the main terminal building. From a security perspective, they are typically treated no differently than any other commercial activity at the airport. Security design considerations should acknowledge the potential for persons to exit from the hotel on or near the airside, or to pass contraband from hotel windows to persons on the airside. While direct sight lines to active aircraft movement areas are often considered an attractive feature of airport hotel design, it is not a particularly desirable feature from a security point of view, considering potential trajectories from a nearby, publicly accessible, private hotel balcony. Other considerations include security design elements to accommodate the hotel cash-handling activities and vendor/supplier traffic at all hours of the day.

6.5.3 Intermodal Transportation Area

As cities and airports expand, mass transit systems are increasingly being integrated into the airport access scheme. The practice of transferring from one mode of transportation to another to reach a destination is termed intermodal transportation. Both light and heavy rail systems are now bringing travelers to the airport, with automated people movers acting as circulators connected to a rail station, which is sometimes elevated with airside sight lines.

When planning, designing, or renovating an airport, alternative modes for moving people in and out of the airport should be considered. When such intermodal alternatives are being discussed, security and safety concerns should also be part of that consideration. For example, public transit generally limits the exposure to a man-portable threat (backpack or duffel) rather than significantly larger Vehicle Borne IED–sized threats.

6.5.4 Rental Car and Vehicle Storage Areas

Rental car storage areas are normally landside, and often are well removed from the terminal and possibly the airport itself. However, as these areas use not only security features such as fences and gates, but also access control and CCTV systems, the considerations should be made for equipment and alarm response connections compatible with those of the airport.

Where these areas are located adjacent to security areas or fencing, then bollards, curbing, or other structures should be planned to prevent vehicles from being parked in locations that would violate security clear zones. The requirement to maintain this security perimeter may also need to be incorporated into the respective tenant's lease agreement, since TSA regulations do not extend beyond the airport proper.

6.6 Access Control Portals

Typically, there are access points through fencing or other barriers for both vehicles and pedestrians. Access points through buildings or walls are typically personnel doors, but may also be guard points, portals, or electronic means or controls. In all cases, the access point type and design may be the determining factor in the effectiveness of the security boundary and control in that area. As such, the number of access points should be minimized and their use and conditions closely monitored.

Portals should be located away from the terminal and other critical infrastructure, such as Air Traffic Control towers or radar systems, so that any means of attack will have minimal effect on critical operations.

6.6.1 Gates

While the number of access points should be kept to a minimum, adequate pedestrian and vehicle access points must be planned for routine use, maintenance operations, and emergencies.

Routine operational gates at an airport are typically those used by police patrols and response teams; catering, fuel, and belly freight vehicles and tugs; scheduled delivery vehicles; and ground service equipment and maintenance vehicles.

Most airport gates used for routine operations are typically 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.

Security Identification Display Area, Secured Area, AOA, and other security boundary gates that are high-throughput are the most likely candidates for automation and electronic access control, as well as candidates for adversarial breach. Refer to Section 10, Access Control Systems of this document for further information.

6.6.2 Roads

Ensure that roadways using access-controlled portals to the airside have adequate maneuvering room for vehicles using the gate. These points may need temporary staging areas for vehicle inspections so that these activities do not hinder traffic flow through the gate.

Access through the portal should not require the use of primary traffic roads to and from the terminal. During heightened levels of security, these roads may become backed up because of vehicle inspections.

6.7 Interior Spaces

When interior walls are used as security barriers, consider not only the wall type and construction material, but also the wall height. When possible, security walls should be full height, reaching not just suspended ceilings, but extending floor to ceiling or slab.

Interior walls may be used as part of the security boundary, with appropriate attention paid to maintaining the integrity of the boundary and the levels of access control to a degree at least equal to that of the rest of the boundary, while still allowing for secure pathways for power, communications cables, etc.

6.8 Exterior Spaces

6.8.1 Physical Barriers

Physical barriers are used to deter and delay the access of unauthorized persons onto non-public areas of airports. These are usually permanent structures that are designed to be an obvious physical barrier as well as a visual deterrent, and can also serve to meet safety requirements.

6.8.1.1 Fencing

For airports, fencing all or portions of the property involves consideration of the desired level of security (i.e., deterring incidental intrusions or preventing forced intrusions), whether some or all of the fencing should be instrumented with alarm sensors and/or video surveillance coverage, the quantities and costs of the fencing including post-installation maintenance, and aesthetic issues.

For fences with sensors, there are issues regarding monitoring of the sensors in the Security Operations Center and responding to intrusion alarms.

When utilizing fencing as a security boundary, care must be taken to ensure that the fence does not conflict with the operational requirements of the airport. Access points through the fence are necessary to allow the passage of authorized vehicles and persons. While the number of access points should be kept to a minimum, the plan must be balanced by providing adequate access points for routine operations, maintenance, and emergencies.

To assist in surveillance and security patrol inspection, fences should be aligned as straight and uncomplicated as possible, which will also minimize installation and maintenance costs.

Security effectiveness of perimeter fencing is materially improved by the provision of clear zones on both sides of the fence, particularly in the vicinity of the terminal and other critical facilities. Such cleared areas facilitate surveillance and maintenance of fencing and deny cover to criminals, terrorists, vandals and trespassers alike.

Suggested clear distances range from 10 to 30 feet, within which there should be no climbable objects, trees, or utility poles abutting the fence line, nor areas for stackable crates, pallets, storage containers, or building materials. Likewise, the parking of vehicles along the fence should also be prevented. Landscaping within the clear zone should be minimized or eliminated to reduce potential hidden locations for persons, objects, fence damage, and vandalism.

Effectiveness of fence construction in critical areas can be improved by anchoring or burying the bottom edge of the fence fabric to prevent it from being pulled out or up to facilitate unauthorized entry. Use of concrete mow strips below the fence line and/or burying the bottom of the fence fabric can also deter tunneling underneath the fence by persons and animals. Mow strips may also reduce security and maintenance personnel hours and costs.

For safety or operational reasons (e.g., presence of navigational systems), some sections of perimeter fencing may not be able to meet standard security specifications. Special surveillance or detection measures may need to be applied to improve the safeguarding of these areas.

More specific information on fencing materials and installation, including the use of barbed wire outriggers, is available in FAA Advisory Circular (A/C) 150/5360-13, *Planning and Design Guidelines for Airport Terminal Facilities*; and Advisory Circular 150/5370-10, *Standards for Specifying Construction of Airports*. Refer also to Fencing (Section 11.3.2) in the Perimeter Intrusion Detection System section of this document for more information.

Note: As this Guidelines document is being finalized, the FAA has released a draft for industry comment reflecting many changes in A/C 150/5360-13A, *Planning and Design for Airport Terminal Facilities*. When published, AC 150/5360-13A will cancel both A/C 150/5360-13, and AC 150/5360-9, *Planning and Design Guidelines for Airport Terminal Facilities at Non-Hub Locations*.

6.8.1.2 Buildings

Buildings and other fixed structures may be used as a part of the physical barrier and be incorporated into a fence line if access control or other measures to restrict unauthorized passage through the buildings are taken at all points of access. Whether those points are located on the airside or landside boundaries, or perhaps through the middle of such buildings, may be dependent upon the nature of the business being conducted inside, and the level of continuous access required by those personnel.

6.8.1.3 Exterior Walls

While often not as economically affordable as chain link fencing, the use of exterior walls as physical barriers and security boundaries is frequently necessary. Walls provide less visibility of storage or Secured Areas, and can be matched to the surrounding architecture and buildings. In addition, some varieties of exterior walls are less climbable and thus more secure than security fencing or other barriers.

Walls of solid materials should not have hand or foot holds that can be used for climbing, and tops of walls should have barbed wire or other deterrent materials. Jet blast 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.

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 Secured Area is maintained to at least the level maintained elsewhere along the boundary.

6.8.2 Lighting

The use of illumination can help deter criminal activity as well as reduce accidents. Key issues are the levels of illumination, the reduction of shadows, and the lighting of horizontal surfaces. Areas for careful consideration include parking structures, stairwells, and pedestrian routes. Lights should be flush-mounted or recessed whenever possible, and covered with an impact resistant material.

It is important to be aware of the line of sight between fixtures and objects in areas that may cast shadows, such as corners, walls, and doors. In addition, consider painting surfaces a light color. This will help reflect light and give the areas a more secure “feel” for people using the space.

6.8.3 Utilities and Related Equipment

Design and location of utilities, and related equipment and service areas, should be coordinated with security and fencing design to minimize security risks and vandalism potential. While it is beneficial from a safety and vandalism standpoint to locate utility equipment in the secure airside when possible, maintenance contract and service personnel ID media issuance and access may require utilities to be landside; although they must then also be secured. Special emphasis should be given to above ground electrical substations and manhole access points outside the perimeter.

Where underground service ducts, storm drains, sewers, tunnels, air ducts, trash chutes, drainage structures, and other openings providing access to the airside or other restricted areas, security treatments such as bars, grates, padlocks, or other effective means may be required to meet practical maximum opening size requirements. For structures or openings that involve water flow, the security design should consider the direction of flow, type, and size of potential debris, the frequency and method of maintenance access required for debris removal, as well as the potential for flood and/or erosion during heavy flow/debris periods.

6.9 Systems and Equipment

6.9.1 Electronic Detection and Monitoring

In the case of boundaries that are monitored by electronic sensors, motion detectors, infrared sensors, cameras and other devices, it is clear that these are intended to serve essentially the same security functions as other detectors, but are simply employing different technologies, usually with somewhat higher maintenance costs. They will often be used in conjunction with other technologies such as alarms, CCTV, or other reporting and assessment methods. Nonetheless, there are appropriate places for such applications, especially where normal conduit and cabling might be impractical, or where excessive trenching might be required.

6.9.2 CCTV

Landside areas accessible to the public are the most difficult to control or monitor from a security standpoint because they must remain accessible to the traveling public and service personnel. Public areas of airports are not normally subject to federal airport security regulations, but during implementation of crisis contingency plans, they can be expected to be affected by special security measures. Prudent use of surveillance technologies such as CCTV and video analytics should be considered in monitoring areas of concern, in consultation with airport law enforcement, the airport security coordinator (ASC), operations personnel, and other local crime control interests. CCTV should be considered for coverage of terminal curbside areas, parking lots/garages, public transportation areas, loading docks, and service tunnels.

6.9.3 Alarms

Airport operators should place duress alarms in restrooms and/or public areas to facilitate police/emergency response.

6.10 Emergency Response

6.10.1 Law Enforcement

Planners should provide for a remote temporary police substation or presence in the vicinity of an incident.

6.10.2 Off-Airport Emergency Response

While first response to many on-airport emergencies—such as fires, medical events or injuries, and traffic accidents—will usually be by on-airport response personnel, local codes, mutual aid agreements, or unusual situations may require response by off-airport emergency or law enforcement personnel. In addition, some airport primary response personnel (such as for structural fires) may be from off-airport organizations, such as Explosives Ordnance Disposal units or nearby community fire/EMT response. Both procedural and design-related coordination must occur, particularly where off-airport response personnel may need to enter security areas. Where special procedures or design elements may be required, planners should assure that they are coordinated with TSA, FAA, local police, fire, and other off-airport organizations during the preliminary design. Incorporation of airside and landside staging areas helps reduce congestion of response vehicles and personnel.

Features associated with off-airport emergency response that can be incorporated into an airport's design include:

- The use of special "agency-only" identification media, PINs, or card readers that provide emergency personnel with access identification media.
- Installation of a vehicle ID system, such as radio frequency identification tagging that enables emergency vehicles to access security areas and be tracked while on airport property.
- Incorporation of screening checkpoint "bypass routes" that provide direct Sterile Area access for escorted personnel and personnel with appropriate ID media without the need to use the public checkpoints. These bypass routes must be sized to provide quick, unobstructed access for police, fire, medical, and emergency response personnel and equipment.
- To facilitate quicker response or to keep airport and off-airport emergency personnel advised of incidents, a linked notification system and/or procedure is desirable. This will allow for added coordination with less risk of secondary incidents and delays. This may be beneficial to off-airport emergency services requiring access through passenger checkpoints, response to major airport-related traffic incidents, on-airport structure fires or medical incidents, and on-airport emergency landings or crashes, which could become off-airport traffic problems.

6.10.3 Life Safety Equipment

Planners should consider incorporation of life safety (emergency medical) equipment, defibrillators, and/or duress alarms in public and restroom areas, and/or at locations where airport personnel deal directly with money, baggage, ticketing, and/or disgruntled persons. Emergency phones or intercoms in public areas and parking areas also should be considered. When possible, life safety equipment, duress alarms, and phones/intercoms should be complemented by CCTV surveillance to assist emergency dispatch personnel.

6.10.4 Emergency Services Coordination

It is important to maintain close coordination with the ASC and to remain aware of any constraints placed upon the airport through the ASP, the Emergency Plan, Homeland Security Directives, and any contingency plans. In addition, the Ground Security Coordinator for each airline should be consulted to ensure that their contingency measures have been considered at the design and planning stage.

6.10.5 Threat Containment Units

Many airports have threat containment units (TCU)—mobile hardened containers where suspect items can be placed for bomb squad response (See Appendix B). TCUs will typically be stored in or very near the terminal. It is important to determine how the responding bomb squad will gain access to the TCU, and how it will be transported throughout the terminal. If manually, it is important to practice moving them to know what challenges might be encountered in an actual situation, especially in the baggage makeup and baggage screening areas. Large TCUs are designed to be hooked to the back of a vehicle and driven away. The TCU can be pushed by as few as four individuals; however, slight inclines can be difficult for maneuverability. Designers should create appropriate TCU access.

6.11 Checklist

Landside Checklist

- □ Monitor areas of concern:
  - Terminal curbside areas
  - Parking lots/garages
  - Public transportation areas
  - Loading docks
  - Service tunnels
- □ Consider life safety measures
  - Duress alarms
  - Emergency phones/intercoms
  - Medical equipment
- □ Landside Roads
  - Minimize proximity to fencing
  - Pre-terminal screening capability
  - CCTV monitoring for security/safety
- □ Landside Parking
  - Terminal Passenger Parking
    - Separate parking lots and terminals
    - Consider CCTV, intercoms, duress alarms
    - Emergency phones/alarms
  - Employee Parking
    - Emergency phones/alarms
    - Airport access control potential
- □ Landside Vulnerable Areas
  - Terminal
  - Utilities
  - Communications
  - Catering facilities
  - Fuel equipment and lines
  - Storage areas
  - Loading docks
- □ Landside Facilities
  - GTSA
    - Security/safety concerns include:
      - Deterrence of vandalism, theft
      - Possibility of terrorist assault
    - Planning/design measures may include:
      - Limitation of concealed areas

        - Provisions for open stairwells
        - CCTV surveillance of area
        - Duress alarms in public areas
        - Minimize congested waiting areas
        - Sufficient night lighting
    - Hotels and On-Airport Accommodations
        - Access to terminal
        - Treated same as commercial areas
        - Limit direct line of sight of aircraft
        - Maximize distance to AOA
    - Intermodal Transportation Area
        - Transit/Rail systems - secured transitions
        - Standoff distance between station and AOA
    - Rental Car Storage Areas
        - Protect vehicles and workers
        - Potential tie-in to access controls
        - Maintain fencing clear zones

- □ Off-Airport Emergency Response
    - Consider access routes, methods and needs
    - Design features may include:
        - Special ID media, PIN for emergency access
        - Emergency Access to terminal area

SECTION 7: TERMINAL

7.1 Terminal Security Architecture

From a security perspective, airport terminals are generally divided into two zones, usually referenced as *landside* and *airside*. International Civil Aviation Organization (ICAO) defines the line of demarcation at the screening checkpoint; the United States typically defines the line to include Secured Areas, Sterile Areas, and the AOA. The security systems and procedures serve to transition the passenger from landside security processes and measures to the airside, where security measures differ significantly: i.e., a transition from land-based transportation systems to air-based systems; a transition in the flow of passenger movement; and a transition in the management of airport operations.

This transitional aspect of airport terminal planning and design means the planners should accommodate some flexibility for various activities on both the landside and airside while permitting efficient and secure methods for operational transition between the two. The complexity of meeting the functional needs of the owners, operators, airlines, and users of an airport terminal requires a combination of transition strategies. To develop appropriate collaborative strategies to meet current security requirements and provide the flexibility for future change, a successful planning and design process requires the participation of an airport operator security committee; fire protection and law enforcement personnel; aircraft operators; the TSA; various state and federal government agencies; tenants on both the airside and landside; and both commercial and private aircraft operators, to develop appropriate collaborative strategies to meet current security requirements and provide the flexibility for future change. This section provides an overview of many of the concepts and methods involved in security planning and design of terminal building facilities. Other sections throughout this document, as well as links to a wide range of other resources, provide considerable detailed guidance for security-related improvements in the airport environment.

7.1.1 Functional Areas

The basic functionality of operational areas within airport terminal buildings has not significantly changed in years. While there are new ways to process passengers and bags through the evolution of automation and technology, the basic functions remain the same. Those processes are likely to continue to evolve during the next several years as better and faster new technologies are introduced, new regulations are required, and airlines modify service levels both up (to accommodate larger aircraft, such as the Airbus A380) and down (to accommodate prevalent economic conditions as well as the continuing proliferation of regional jets). The goal of this section is to assist the airport terminal designer in understanding the need for flexibility and adaptability in considering these wide ranging and fast changing security requirements, including inside, between, throughout, and around multiple terminal buildings. Some design attention must also be given to meeting current regulatory security requirements, but also include some flexibility to allow the next designer optimal opportunity for upgrades and modifications.

Each airport has a unique road system, architectural design, and both structural and operational philosophy. Further, those architectural components collectively interact in almost every aspect of facility design. Each airport operator should tailor its security design solutions to resolve its fundamental security vulnerabilities and meet operational needs. Airport planners, architects, and engineers might consider implementing the following design strategies:

- Approach roadways and parking facilities that have adequate standoff distances from the terminal
- Blast resistant façade and glazing materials or fabrications
- Surveillance systems (such as CCTV cameras, video analytics, microwave, etc.) at curbside, doorways and perimeters
- Structural columns and beams that are resistant to explosive blasts and progressive collapse
- Vehicle barriers that prevent vehicle-borne IEDs from driving close or into the terminal
- Capability for vehicle inspection stations with ample space for vehicle queuing and standoff distances

While each of these design features is individually beneficial, the combined effect of such features can offer significant security improvement. Airport operators and airport designers should recognize the benefit derived by incorporating secure design features, including passive measures that offer protection regardless of the nature or level of threat.

7.1.2 Physical Boundaries

Airport terminal configurations can vary widely, so the implementation of various security measures can take many forms in response to airport planning, programming, and regulatory issues. One criterion that is common to all is the typical requirement for a physical boundary between differing levels of security, such as between non-Sterile Areas and Sterile Areas. Standard building structures such as walls and partitioning typically provide most of this physical separation, although in the case of screening checkpoints and CCTV surveillance, see-through lines of sight should be considered. Large public assembly facilities such as terminal lobbies normally have the architectural characteristics of openness, spatial definition, and circulation. Architectural planners and designers have been innovative in successfully blending these requirements to create secure facilities.

For further discussion on specific design aspects of boundaries and barriers such as walls and doors, see sections in this document on Airport Layout & Boundaries (Section 4); Landside (Section 6); Passenger Screening (Section 9); Access Control (Section 10); and Video Surveillance (Section 12).

Areas that are unmonitored by technology, or are easily accessible to the unscreened public, must provide higher levels of security boundary definition and control than monitored areas such as security checkpoints. Where boundaries are solid (floor to ceiling), security strategies are primarily concerned with access points through the boundary. Boundary surfaces must be capable of preventing the passage of objects or weapons.

Where the boundary surface is not the full height of the opening, the boundary must be capable of preventing objects or weapons from being easily passed over, around, or through the boundary and across security levels.

At security checkpoints, it is useful to have a means of closure for the entire checkpoint area during overnight periods and unscheduled or emergency operations. In such instances, roll-down divider walls and gates should be substantial enough to direct passenger and public movement and deny passenger contact across the security boundary. Boundaries may also be used to contain passengers on the Sterile side of a security checkpoint for a brief distance to reduce the potential impact of a security breach, as well as to provide a visual or psychological deterrent to keep unauthorized persons away from nonpublic areas.

7.1.3 Bomb/Blast Analysis Overview

Blast analysis and mitigation treatments are addressed at greater length in Appendix B. During heightened threat levels, vehicle access and parking near the terminal can be limited, and vehicle inspections are often implemented. To justify driving or parking close to the terminal, a Bomb Incident Protection Plan can be developed by the airport operator.

Blast analysis should be an integral part of the early design process for the airport terminal, roadway layouts, transit station, and parking facilities. It is important that considerations for blast-resistant placement and orientation as well as integral design features that reduce risk and injury due to a bomb blast, or limit available areas to conceal a bomb, be considered early in the design or renovation. The cost of incorporating blast resistant features in the initial design is often much lower than when these are implemented later as a retrofit.

The primary objective for developing a mitigation analysis is to minimize damage by limiting the amount of primary structure damaged in a blast. In short, a blast analysis predicts the structural damage incurred when bombs of various sizes are detonated at different distances from the terminal building. The analysis focuses on evaluating the primary structure—columns, girders, roof beams, and other lateral resistance systems.

- When developing and evaluating blast resistant solutions, it is important to:
    - Define the threat(s)
    - Establish performance objective(s)
    - Develop conformance solution(s)

  For example, if the threat is defined as a Vehicle Borne IED (VBIED), the performance objective is “collapse prevention” and the solution may be to provide blast resistant columns along the curbside of the terminal building. Further, a VBIED is defined as a vehicle in motion, presenting a greater and somewhat different threat than a vehicle with no driver, such as a parked car, which is known as a “placed” IED. Clearly, columns are not the only viable solution; each airport operator should choose the approach they believe is best for their respective facilities.
- Priority should be given to implementing blast protection measures that:
    - Are passive (and do not rely on personnel)
    - Do not hinder airport operations and functions
    - Consist of durable materials (will not fade, discolor, or become brittle with time)
    - Do not distract from terminal architecture and aesthetics
    - Provide cost-effective improved blast protection
- Airport blast protection measures can be separated into two basic categories:
    - Structural—these are blast mitigation measures that can be employed to enhance the protection envelope around the terminal or reduce the need for vehicle inspections. Blast hardening the perimeter columns of the terminal is an example of this type of feature.

- Non-structural—these are blast-resistant features that offer some measure of blast protection, but have no effect on the need to inspect vehicles or restrict parking during heightened threat levels. Installing blast-resistant window treatments and strengthened and/or non-fragmenting trash containers are examples of this type of feature. Some window glazing enhancements provide a balanced approach with framing tied into the surrounding structural members.

In lieu of incorporating blast resistant solutions in the terminal design, airport operators may elect to inspect vehicles approaching or parking near the terminal. A "vehicle inspection" methodology is generally acceptable and viable when heightened threat levels occur. However, this expensive labor-intensive solution tends to be more appropriate for very short periods of time, and when heightened threat levels occur infrequently. Over the long term, using vehicle inspections as the primary mode of security has significant drawbacks, such as delay and traffic congestion, high inspection manpower costs, and lost parking revenue.

One must recognize that the layout, roadway, and architecture of many existing airports are not conducive to implementing certain blast resistant solutions. Also, the airport site might be constrained and not allow much standoff distance between a potential VBIED and the terminal building. While parking above, below, and directly adjacent to the airport terminal building offers great convenience for passengers, many parking locations are troublesome from a blast vulnerability perspective.

There are methods to retrofit existing columns, walls, and floors to resist blast pressures and catch or deflect debris. One should compare the cost of this type of retrofit against the life-cycle cost of a long-term vehicle inspection solution, bearing in mind the findings of a threat and vulnerability analysis, which may suggest a balance that mixes both approaches over time.

7.1.4 Limited Concealment Areas/Structures

This topic has been referenced previously in Section 7.4, Public Areas. Wall configurations, built-in fixtures, freestanding elements, and furnishings should be designed to deter the concealment of parcels that may contain explosives or other dangerous devices. This is particularly applicable to public areas, such as ticket counters, lobbies, seating areas, or baggage claim areas.

Spaces such as storage or custodial rooms that may border or provide access from public areas to Sterile or Secured Areas should have locking doors. Areas that are accessible, such as restrooms, should also be designed to minimize the ability to conceal dangerous devices.

Where structures with concealable areas are unavoidable, planners should consider designs that are easily, quickly, and safely searchable. Furnishings and structural design should be coordinated with local security, search, and threat response agencies to ensure it meets their requirements, and that such spaces are included in all search protocols. Reduced search times can minimize airport downtime, passenger inconvenience, and negative publicity.

7.1.5 Operational Pathways

Efficient terminal facilities do much more than move persons and baggage through various spaces. A tremendous amount of behind-the-curtain activity must occur in support of passenger activities for the whole process to function smoothly. Much of the support activity occurs in areas and pathways that are out of public view and have no public access. Aircraft operator and airport personnel need access to various functions of the terminal on a continual basis, sometimes at a hectic pace. Concessionaires within the terminal should have a means of delivering supplies and materials to various locations without impacting passenger circulation. Airport system monitoring and maintenance functions need to occur away from passengers whenever possible.

Access to and the security of service corridors and nonpublic circulation pathways requires coordination of the architectural program, aircraft operator functions, and terminal security design. Use of corridors that provide access among multiple levels of security in the terminal should be avoided but, if necessary, particular attention should be placed on the control of access to and along the corridor portals. Access points should be minimized.

Vertical circulation can be particularly problematic since building functions and levels of security are often stacked. Code-required exit stairs often double as service corridors, requiring particular attention to security strategies along their length. Exit stairs should only egress into public areas. Uncontrolled exits to the AOA should be avoided. Elevators have very similar issues. Public elevators should not cross levels of security, although service elevators, by operational definition, typically access all levels, and may need access controls in some areas or some higher/lower levels, considering not only exits, but lines of sight or where it is possible to pass items over balconies. Access controls in the elevator can be programmed to allow or disallow access to individual levels.

Airport police and other law enforcement entities often need secure nonpublic corridors to escort persons between aircraft or various public areas of the building and the terminal police holding areas. Terminal police stations should have direct access to the service corridor system for this transport. Likewise, airport police stations should have direct access to nonpublic parking areas when vehicular transport becomes necessary.

7.1.6 Minimum Number of Security Portals

Architectural design should minimize the number of security portals and pathways, both to reduce costs and the potential for a breach. This can be done through the use of service corridors and stairwells that channel personnel from various areas prior to entrance into the SIDA or another security area.

Architectural planning and design can develop several areas of security within the terminal and develop boundaries between them. The dynamics of airport operations require that all boundaries have strategies for transition across them. The best method is to limit the number of access points to the minimum number acceptable for operational requirements. If possible, planners should concentrate nonpublic circulation prior to access through a security boundary similar to a public checkpoint. Code-required public exit pathways should be from higher to lower levels of security whenever possible. If code-required exits must egress to an area where higher security is imposed, such as from hold rooms to the SIDA, architectural design should accommodate control and monitoring by the security system.

In some instances, an automatic door in a security boundary might be considered, bearing in mind there are some safety and maintenance challenges. A large cross-sectional area may require an oversized entry such as a roll-up door. The operation of such an entry should be integrated with the security system so that permission is required to open the door and that closure or alarm is automatic after a programmed delay.

7.1.7 Space for Expanded, Additional, and Contingency Security Measures

Architectural planning and design usually considers contingencies for future growth and expansions of a terminal facility. Planning is done for expansions of public and support spaces, growth and distribution of airport systems, location or expansion of future security checkpoints, and additional measures needed during periods of heightened security. Incorporation of additional space and utility terminations for expansion and contingencies reduces cost for the later installation and execution of those measures. It also minimizes the operational impact when those measures are added, but may impact alternative interim uses for the space, such as concessions.

Heightened security levels may require the addition of temporary or relocated checkpoints to facilitate enhanced security processing. This may involve preparing the utilities infrastructure for additional CCTV monitoring of landside and airside areas. Airport Emergency Command Post (CP) areas will be activated and may require additional or remote sites, along with the requisite wiring and related security equipment. The terminal roadway system may require the accommodation of temporary guard stations at the curbside or other critical approach areas, with a need for additional communications and perhaps heating or cooling. Communications and data systems may require temporary expansion and/or remote input capability, possibly by wireless connectivity. Concession spaces within Sterile Areas may need to be relocated to non-Sterile Areas.

Because space is at a premium at an airport, areas designated for contingency use could also serve other purposes, such as public lounges, children’s play areas, local artifact or commercial displays, etc., bearing in mind any added security measures and boundaries if the need arises.

Early discussions with the Airport Security Committee, security consultants, and airport planners will establish the level of activity and types of expanded, additional, and contingent security measures to be incorporated in architectural design efforts.

7.2 Terminal Area Users and Infrastructure

7.2.1 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, 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) and Immigration and Customs Enforcement (ICE) 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, but are nonetheless 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. Section 10, Access Control Systems deals with those permissions.
- 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 on the public, Sterile, or Secured side of screening, 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 Airport Security Program (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 may or may not have specialized security design requirements, depending on their types of operations and their location in relation to other Secured Areas and facilities. Some airports have light industrial zones where the main operations occur outside 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 general aviation (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 includes 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.

7.2.2 Personnel Circulation

The security designer faces a challenge to provide ease of personnel circulation in the terminal. Many terminal buildings present additional challenges by incorporating vertical circulation with elevators, escalators, and stairwells that service multiple levels on the public side. Circulation must be enabled with a view toward the boundaries of Sterile or Secured Areas, particularly those leading to and from administrative areas, boarding gates, and passenger hold-rooms, as well as at baggage claim areas where carousels and doors may provide a direct path between public and Secured Areas.

When considering circulation from a security design perspective, it is important to move people quickly and efficiently from one public location to another, and to keep them from moving into any area that is, or leads to, a Secured or Sterile Area. This may involve design solutions such as physically separating people along non-intersecting paths of travel, or it may require methods of access control or directional channeling. Circulation must provide an optimal amount of appropriate employee access, while not compromising security. Finally, attention must be paid to circulation resulting from emergency operations, so that evacuees are channeled away from Secured Areas.

7.2.3 Utility Infrastructure

Security aspects of the planning, design, and architectural considerations that support necessary utilities in the terminal are discussed in Section 13, Communications, IT, Power, & Cabling; as well as measures in Section 10, Access Control Systems; and Section 12, Video Surveillance, Detection, and Distribution Systems, among others.

7.2.4 New Construction vs. Alterations

While there is an important distinction between the two concepts of new construction versus major (or even minor) renovations to an existing building, there is no significant difference from a security standpoint regarding the standards that must be met. No matter what changes are made to an existing building (renovation and/or expansion), or what features are provided in a newly designed terminal, they must meet all security requirements, both regulatory and operational. Security alterations to an existing building may also be impacted by building codes and result in added modifications and increased costs.

An existing building may have physical constraints that make a particular security concept difficult or impossible to retrofit. One example might be a curved or angular concourse that provides very limited lines-of-sight for surveillance. Such constraints may require the designer, in consultation with the airport operator, to choose an operational alternative that may not be the optimal choice. That choice may be further defined by such factors as initial cost and funding sources, short- or long-term maintenance concerns, compatibility with related legacy systems such as access control or CCTV, their associated cabling and power capacities, and the projected lifespan and/or future changes associated with the building that is being redesigned.

Indeed, those same factors, and possibly others, may drive similar decision-making processes during the design of a new terminal building. The difference is that while the constraints of an existing facility may no longer be a limiting factor, the clean slate of a new facility design allows for many more technological and procedural options, each of which may bring many more competing design influences to the table, along with added costs and integration challenges with legacy systems. For example, in updating an existing building, one may consider retaining the same doors at the existing locations. This could enable using existing cable routings, equipment closets, and perhaps the same access control and CCTV technologies. A new facility, however, provides a multitude of options for new vertical or horizontal circulation patterns, new entries and exits, new demands for added terminal building infrastructure requirements (i.e., power, water, HVAC, etc.), and new technologies, which may out-perform existing ones and put into motion future plans for upgrades of legacy systems to meet new standards.

In summary, each terminal building project requires a similar decision-making process to determine the appropriate security requirements, and how they are to be applied. This would occur in the development of a Concept of Operations (ConOps), which examines the airport security requirements and the available options. This would apply to new and renovated or expanded structures. The final decisions and outcome for each project will be very different. This document can help guide the designers through the process.

7.3 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 security screening checkpoint 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 the TSA screening protocols and 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 security screening checkpoint and prior to boarding an aircraft. 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 security screening checkpoint. 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. Doors must also comply with applicable local fire and life safety codes and Americans with Disabilities Act (ADA) requirements, among others. Guards are generally an expensive alternative to technology in this application. Discussions with local building and/or life safety code officials should take place early to resolve special design issues, including how to accomplish the securing of 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, or other channels.
- When planning the construction of non-Sterile or public access to 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 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 nonpublic, easily accessible, never blocked by storage boxes, bins, or other hazards, and provide clear, quick access for any emergency equipment needed (e.g., stretchers, wheel chairs, explosive detection devices, transportation equipment, or paramedic equipment, etc.) Routes (and access controls) to accommodate off-airport response (emergency medical services [EMS] 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 usually located within the Sterile Areas. Concessionaires and other airport tenants 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. 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.

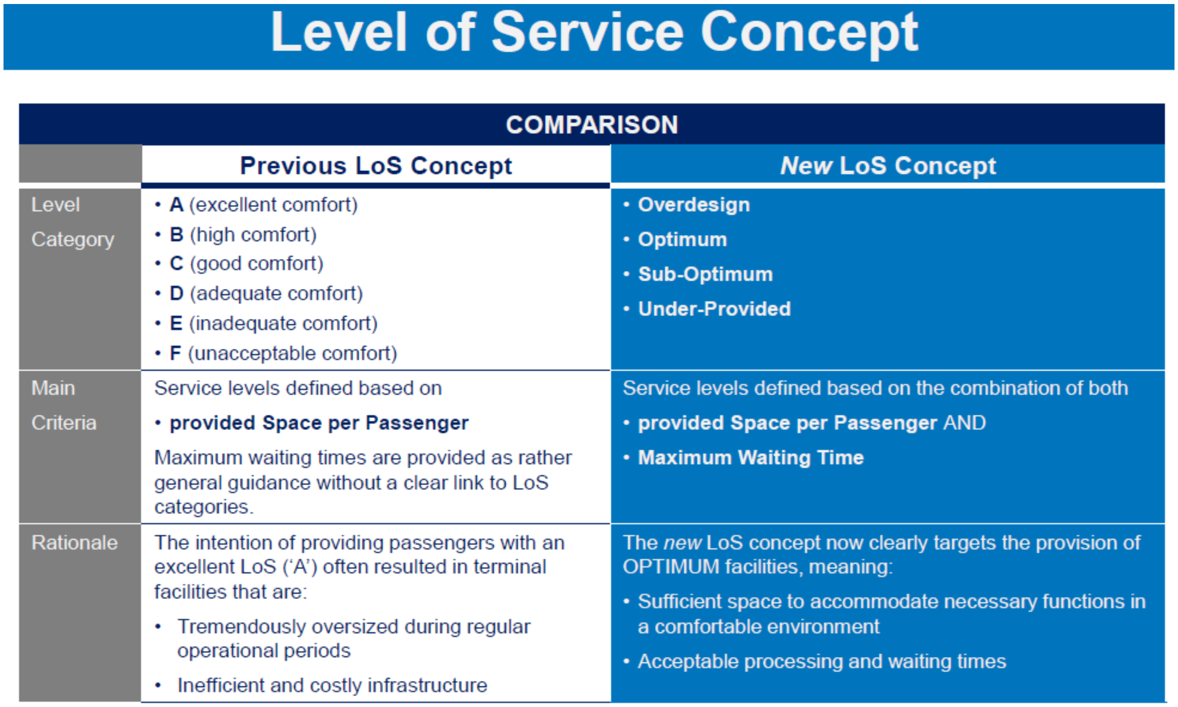
- During construction or modification of facilities, provisions should be made to ensure that any individual who has not undergone screening is prevented from having contact with a screened person inside the Sterile Area.
- Security of Sterile Areas is improved with design solutions that deter the concealment 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.

7.4 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 (LoS) concept in passenger terminals is generally discussed in terms of space requirements—whether the passengers will fit in that 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.

IATA's *Airport Development Reference Manual* is a good guideline to define LoS. The IATA concept was completely revised in late 2015 to reflect the dynamic nature of terminal throughput with two important quantitative and qualitative variables—space and waiting time—in four categories: under-provided, sub-optimum, optimum and over-design. While LoS is not a direct determinant of security design, it must nonetheless be kept in mind when, for example, transitioning in, out, and through areas with differing levels of security, and particularly in such areas as narrow concourses where checkpoint queuing interferes with other public throughput.

Table 7-1. IATA's Level of Service Concept



Level of Service Concept

COMPARISON

	Previous LoS Concept	*New* LoS Concept
Level Category	• **A** (excellent comfort) • **B** (high comfort) • **C** (good comfort) • **D** (adequate comfort) • **E** (inadequate comfort) • **F** (unacceptable comfort)	• **Overdesign** • **Optimum** • **Sub-Optimum** • **Under-Provided**
Main Criteria	Service levels defined based on • **provided Space per Passenger** Maximum waiting times are provided as rather general guidance without a clear link to LoS categories.	Service levels defined based on the combination of both • **provided Space per Passenger** AND • **Maximum Waiting Time**
Rationale	The intention of providing passengers with an excellent LoS ('A') often resulted in terminal facilities that are: • Tremendously oversized during regular operational periods • Inefficient and costly infrastructure	The *new* LoS concept now clearly targets the provision of OPTIMUM facilities, meaning: • Sufficient space to accommodate necessary functions in a comfortable environment • Acceptable processing and waiting times

Source: IATA ADRM

Key to this is the variation in bags per passenger, or carry-on items per passengers as they circulate throughout the terminal and queue at the checkpoint. There is also variation based on the segment of traffic (e.g., international or domestic) that could lead to more congestion. For general planning purposes, a good level of service under the previous guidelines would provide somewhere between 13 and 22 square feet per passenger. However, detailed tables in the new IATA guidelines reflect a range of values for space and waiting time to allow the airport to tailor its service levels to the market and region it serves.

7.4.1 Configuration of Lobby Areas

Security is improved by reducing congestion and long queues at the curb and in public lobby areas. Large concentrations of passengers in the public areas not only reduce the level of passenger service caused by limiting free movement, but can become a threat target. Promoting the free flow of passengers requires adequate capacities at each successive stage, including curbside check-in, ticket counters, screening checkpoints, and vertical transportation that 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 by coordinating with the time passengers spend going through passenger screening to avoid excessive queuing at either location.

7.4.2 Configuration of Domestic Baggage Claim Areas

The current designs of the claim areas for baggage arriving on domestic flights include vulnerabilities that can be addressed in new designs. Such features as claim areas accessible 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 flights are completely within the airports' Federal Inspection Service (FIS) Secured Areas where no unscreened persons or bags enter. They are not accessible from the street. Arriving passengers move from the aircraft to the claim areas without leaving the Sterile Area, claim their bags, process through Customs and Immigration, and then exit to the public area to leave the terminal. International baggage claim is much less susceptible to unwanted contact or access.

Airports may want to consider whether the design of baggage claim areas and the routing of arriving passengers should be similar for international and domestic arrivals. (International arrival areas must also accommodate FIS functions, which domestic arrival areas need not do.) 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, the secure (international) layout of baggage claim areas can 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. Exit lane technology is described in greater detail in Section 9, Passenger Screening Checkpoint.

Planners should consider ways of differentiating between public and Sterile or non-public areas in terminal design to deter unauthorized entry. Segregation of these areas requires a capability to secure or close down Sterile Areas not in use, and possibly CCTV surveillance coupled with motion detection to maintain vigilance while unattended.

When selecting architectural and other built-in fixtures and furnishings (e.g., trash receptacles, benches or seats, pillars, railings) for the terminal, avoid those likely to facilitate the concealment of explosives or other dangerous devices, or those likely to fragment readily, such as aggregate cement/stone trash containers. Avoid locating or attaching trash containers and newspaper vending machines to structural columns, because the columns could be damaged significantly if in close proximity to a detonated explosive device. When possible, deny places to conceal IEDs, incendiary devices or weapons. Typical hiding places in the past have been restrooms and public lockers, closets, utility rooms, storage areas, stairwells, and in recessed housing for fire extinguisher or fire hose storage. Closets, utility rooms, access portals, and similar enclosed spaces should be locked when not attended.

If assessments by airport security officials or a prior history of incidents indicate an airport is at increased risk of explosive attacks, planners of new facilities should seek advice from structural and explosives experts. A Bomb Incident Protection Plan and vulnerability assessment should be developed in accordance with DHS/TSA guidelines.

Advances in technology continue to bring about new ways of doing business. Some airline passengers may check in at a remote location, such as online, a hotel ticket office, or a cruise ship terminal. Most airlines now offer an electronic ticketing or boarding pass option, in which checked baggage might not be handled in the usual fashion at the airport ticket counter. Architects and planners should consider the requirement to maintain the security of checked baggage arriving through non-traditional airport processes, perhaps through such approaches as additional curbside check-in locations. This concept revolves around a secure "chain of custody" in which control of the baggage must be maintained throughout the system, from the moment the passenger relinquishes it to the point where they regain it.

Seating in public areas should be kept to a minimum to reduce congestion, encourage passengers to proceed to the gate areas, and facilitate monitoring and patrolling of public areas. Obviously, if landside seating is denied in order to keep people moving, there should be adequate seating available at their various airside destinations.

Careful consideration should be given to the needs of specific aircraft operators, particularly international, who may need to apply additional security measures and passport controls during the passenger check-in process. Additional queuing, secondary screening and interview space may also be required.

7.4.3 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 might compromise optimal security planning. Without appropriate planning and design, emergency exit requirements can yield doors that provide inadequately secured access to Secured 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/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 actual emergency or when a concourse may have to be cleared when a breach has occurred. 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 having push-type panic bars with 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 CCTV, and monitored door alarms can drastically reduce the consequences of false alarms and the need for officer dispatches and other responses to security breaches.

7.4.4 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.

A key component of the physical security system within the FIS area of an international arrivals terminal is the installation of delayed egress and CCTV monitoring capability on all emergency exits. The FIS area must remain Secured and Sterile to prevent smuggling of illegal aliens, terrorists, criminals, and contraband into the United States. Guidance on FIS design requirements is found in the Appendix C; security requirements for the FIS area are included in the CBP *Airport Technical Design Standards*.

7.4.5 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. Enhanced security requirements suggest revisiting the balance between locating more concessions in the Sterile Areas, close to the hold rooms where only passengers are allowed, and placing concessions in public areas ahead of security screening checkpoints, where persons without boarding passes can contribute to the revenue flow.

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, CCTV, 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 frequencies 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 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 both 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.

7.4.6 Signage

Having clear, easily understood signage is important for accommodating the control and expeditious flow of passengers, greeters, tenants, contractors, and airport support personnel and their vehicles during normal operating conditions, and especially during emergency and security-related conditions.

Airports will generally have locally established policies and style manuals that govern the type and use of structures, materials, colors, typefaces, logos, directional symbols, and other characteristics of signage. Wayfinding signage, a primary element of customer service, includes directories, airline signs, concession signs, flight information displays (FID) and multi-user flight information displays (MUFIDS), regulatory signs, and construction and advertising signs.

In addition to airport preferences, signage must take into account safety and security requirements of the FAA and TSA, certain standards of the DOT and state transportation departments, and requirements of the ADA, among others, including airlines and other tenants, particularly in common-user areas.

It is critical that the designers of any security information system completely understand the operational and functional goals of the architectural and security environment. The analysis of vehicular and pedestrian traffic flow, decision points, destinations, potential congestion areas, message conflicts, and common nomenclature provide the designer with a basis for programming the signage plan. The TSA's own security signage options may be obtained through the FSD. These elements are important to security because they convey information needed to understand the paths of travel available, especially when conditions are changing from normal to emergency mode. A comprehensive information system can help to make the security process more user friendly, particularly among new or infrequent users and people with disabilities.

Signage can be classified as either static, such as directional symbols and room labels, or dynamic, which includes constantly updated directories such as FIDS and MUFIDS displays. Integrating dynamic signage with the airport's information systems network can give the airport great flexibility in determining what is displayed at any particular location and at any given time.

This flexibility can also serve security purposes, because dynamic signage can provide the means for delivering security information on a timely basis during rapidly changing security events and emergency situations when fast-changing warnings and instructions for passengers and support personnel are critical. To be effective, these capabilities should be identified early in the planning and design process to ensure that adequate bandwidth and cable plant terminations are provided. It will also be necessary to provide the airport's Security Operations Center with the technical ability and operational authority to control what, where, and how information is routed to interior and exterior signage during such conditions.

There is a wide variety of static signage media available to handle security messaging requirements. However, as information dissemination becomes more complicated due to the complexity of facilities, ingress and egress options, and an abundance of information requirements in the multilingual global environment, the limitations of static signage are quickly realized. Electronic information displays are becoming a keystone to provide flexible and comprehensive directional, destination, and regulatory information, either pre-programmed or in real-time response to changing conditions such as during an emergency evacuation generated by a breach of security. Their accommodation within the information systems design of the airport has become equally critical. It is also necessary to be certain of adequate consultation and coordination with groups representing persons with disabilities, government agencies such as TSA, FAA, and FIS facilities, and those administering local fire and safety codes.

Signage-specific coordination will be required for:

- Electrical and IT systems (providing power and data to signs)
- Video/cameras (obstructions)
- Sprinkler systems (obstructions)
- Lighting (obstructions and/or external illumination of signs)
- Emergency UPS/generator during power loss or evacuation operations

7.4.7 Public Lockers

At present, TSA does not allow the use of public lockers within the Sterile Area or terminal front areas, i.e., in front of the checkpoints. Airport operators with lockers, whether in use or not, should consider eliminating them or subjecting them to constant surveillance, venting any potential blast effect upward rather than outward, as well as adding structural enhancements to the surrounding area.

7.4.8 Unclaimed Luggage Facilities

Consideration should be given for the establishment of facilities for passengers to reclaim unclaimed luggage. The facilities should be on the landside of the passenger screening checkpoint to facilitate ease of access. In addition, access routes for bomb squads and law enforcement agencies should be considered.

7.4.9 VIP Lounges / Hospitality Suites

Some airports feature VIP lounges and/or airline hospitality suites, which are usually located beyond security screening checkpoints in the Sterile Area. Access to these facilities from the Sterile Area is generally limited to authorized personnel and passengers who have passed through the security screening checkpoint.

7.4.10 Vertical Access

Plans should include preventing the traveling public from accessing the airside through connecting elevators, escalators, and stairwells.

7.4.11 Observation Decks

Observation decks accessed from the public area are strongly discouraged. Where these exist, they should be closed to public access. Observation decks accessed from the Sterile Area present less concern, because occupants will have passed through a security screening checkpoint before accessing the observation deck. Any open-air observation decks should deny access to the AOA.

7.5 Non-public Areas

7.5.1 Service Corridors, Stairwells, and Vertical Circulation

Public areas, Secured Areas, and Sterile Areas that are separated in the horizontal plane may overlap in the vertical plane. Even in the horizontal plane, service corridors may transit a portion or the entire length of the terminal. To avoid opening portals for 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 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.)

Service corridors may also be used to minimize the quantity and types of security access points. If access requirements are clustered by similarities of 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 non-service corridors should consider their placement and possible use by airport emergency personnel and law enforcement agencies. While use of service corridors by emergency and Law Enforcement Officer (LEO) personnel 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.

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 are shared for egress and operational movement.

7.5.2 Airport and Tenant Administrative/Personnel Offices

Airport, airline and tenant personnel require support space throughout the terminal facility for various functions. Types of airport personnel offices typically located within an airport terminal include airport administrative offices, maintenance support offices, law enforcement, ID offices, and security force offices and substations, as well as airline and tenant (including government agency) offices.

Office areas are best located close to the primary activity of the occupants 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 should be located and 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 or 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 CCTV 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 design considerations include: security of airport personnel and financial records; security of access control and ID workstations; security of ID media stock and records; safe and money storage areas; and computer server and IT/communications equipment areas, especially for security-related facilities such as the access control and CCTV systems.

7.5.3 Tenant Spaces

There is no fixed rule on whether tenant spaces require tie-in to the access control system. Indeed, there are currently no such regulatory requirements for tenants to have a security program, although if the airport wishes to include tenant areas, it is wise to design a single unitary 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.

7.5.4 Law Enforcement and Public Safety Areas

Guidance materials encourage the provision of security to supporting services at airports serving civil aviation. ICAO Annex 17 contains *Standards and Recommended Practices*, and ICAO Document 8973, *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference* contains extensive operational and procedural guidance. Although the United States is a signatory to ICAO, these are minimum recommendations not specifically addressed by TSA regulations, which are generally more stringent.

7.5.4.1 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 of needs 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 to widely separated facilities, as well as reduce vulnerability to a single point of attack.
- Physical infrastructure should consider adequate space 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. In addition to special consideration for such additional secure communications technology as National Crime Information Center (NCIC), FBI, federal task forces, and other liaisons, attention should also be given to the amounts of conduit required to accommodate future expansion in this era of rapidly increasing security requirements and government liaison.

7.5.4.2 Law Enforcement Parking

Quickly accessible parking for law enforcement vehicles is invaluable to improving response capabilities. When possible, parking should have direct controlled landside/airside access with dedicated spaces and quick access capability in both directions integrated with the access control system. Consideration should also be given for EMT helicopter pads to be located in secure areas, including secured and structurally adequate rooftops, if appropriate.

7.5.4.3 Remote Law Enforcement/Public Safety Posts/Areas

- In large facilities, remote areas, or where minimized response time is a concern, planners should consider the use of remote law enforcement posts or substations. Such locations should be securable, equipped with communications and emergency equipment, and contain a concealed duress alarm when possible.

- When security personnel are deployed to outdoor posts, shelters are needed to provide protection against the elements. Shelters should permit maximum visibility over the immediate area as well as easy access for guards.
- If the terminal building is large (over 300,000 square feet of public area or with large open distances of 2,000 feet or more), storage areas for tactical supplies and equipment should be distributed in tactically identified areas.

7.5.4.4 Other Considerations

- Communication/dispatch facilities, equipment repair areas, and other support tasks near the police functions should be located away from high threat areas and be considered for protection and control treatments.
- Many airports, because of size, activities, budget, and political or joint working arrangements with local police organizations, may combine or contract out some security activities. This does not reduce their need for operational space and equipment, and indeed may increase the need for inter-jurisdictional communications, emphasizing the requirement to have in-depth discussions with all affected security and police officials well before designing their integrated space.
- Airport operators should consider maintaining control of un-issued ID media stock, access control paper records, master keys and key control systems, and the ID office itself by putting them behind a door with a card reader to monitor access to the system and its records, especially during off hours. It is prudent to consider providing secured portals and card readers for any facilities where the airport may wish to have workstations with security system access, particularly where the ID media stock and personnel data may be stored.

7.5.5 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 not actually performing explosives detection duties, but either waiting for an assignment or in training exercises. The canine environment should include an administrative area that houses the dogs’ handlers. While a set-aside training area would also be helpful, it is common for K-9 teams to undertake training exercises at such daily operational areas of the airport 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:

- Adequate ventilation, cooling, heating, and sanitation systems.
- Provide isolation from jet fuel fumes, since the dog's sense of smell is critical to its mission.
- Minimal noise levels. 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 free of infestations of mosquitoes, ticks, rodents, or other pests.
- Must be located in an area that will allow for the proper supervision, protection, and care of the canine.
- Administrative area should have secured storage for training items such as luggage, K-9 supplies, etc.
- Storage facilities 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.
- Also consider reasonable proximity to bomb squad/Explosive Ordinance Disposal (EOD) personnel, as well as adequate parking nearby for K-9 transport vehicles.
- Additional assistance regarding different 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.

7.5.6 Service Animal Relief Areas

Service animal relief areas 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 public landside, not airside, but artificial materials may be used for service relief areas located on the secure side.

Individuals with disabilities will often be able to use these landside areas for their service animals. However, 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 on the Sterile side (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 designated Service Animal Relief Areas, and the circumstances in which access will instead be afforded to other outdoor areas. For transiting/connecting travelers needing access to those service relief areas located inside the Sterile Area, an appropriately badged escort will be required.

7.5.7 Security Operations Center

A Security Operations Center (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 may co-locate with other operational functions. Such designations may include: Airport Communications Center, Airport Operations Center, or Security Control Center. See also Section 15, Security Operations Centers and Command & Control.

An SOC can provide multiple communications links to the airport operator including police, fire, rescue, airport operations, crash/hijack alert, off-airport emergency assistance and a secure communications channel, as well as 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.

A successful SOC typically consists of a multi-bay console, video displays, monitors, controllers, and communications connections (telephone/data, intercom, and radio), all of which have significant design implications for floor space, cabinet space, power, HVAC, fiber optics and other cabling, and conduit paths. Rear access space to the console is necessary for equipment installation, maintenance, troubleshooting, and upgrades.

Connecting all airport security sensors to the SOC requires verification of the connectivity and operability of each of the sensors. Sensors can periodically be commanded to go into alarm states, with the response checked at the SOC panel. This feature could effectively guard against an adversary tampering with or disabling the sensors.

SOC location has a significant effect upon its utility. Ideally, it should be located close to the Airport Emergency CP and in a security area, because the Emergency Operations Center (EOC) must manage the emergency while the airport operator deals with continuing regular operational concerns, and each must coordinate with the other. From the standpoint of cabling interconnections, a relatively central geographic location serves to maintain reasonable cable lengths to all of the detection devices in an airport security system that report alarms to the SOC. In addition, if facilities other than the SOC handle the airport's non-security communication functions (information, paging, telephones, maintenance dispatch, etc.), co-location or geographical placement of the SOC and the other facilities should be considered such that cabling, equipment, maintenance, and emergency operations can be installed, operated, and maintained in a cost-effective manner.

Other communications functions, equipment, and operational areas may be co-located with the SOC. Planners should consider the merit and operational impact of consolidating the following functions within or adjacent to the SOC:

- Access terminals for law enforcement informational systems such as Computer Aided Dispatch, NCIC, etc.
- Automatic notification system for emergency response recall of personnel
- Direct phone lines to ATCT, airlines, local hospitals, and other sites
- Airport Emergency CP
- Fire alarm monitoring

- FIDS systems, Baggage Information Display (BID) systems
- ID management department
- Information specialists for customer information lines, courtesy phones, and airport paging
- Landside/terminal operations
- Maintenance control/dispatch or alarm monitoring (includes energy management of HVAC systems)
- Monitoring of public safety, duress, or tenant security alarms
- Personnel call-down paging system
- Police and/or security department
- Radio systems
- Recording equipment
- Weather monitoring/radar/alert systems
- Network operations monitoring and intrusion detection

7.5.7.1 Airport Emergency Command Post

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 with two or more highly diverse locations for very different events having very 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 needs of 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, either on a fully dedicated basis or with the capability to be rapidly converted and organized as a CP, such as space in adjacent conference or meeting rooms.

7.5.7.2 Location

Site selection for a CP should emphasize communications capabilities, convenience, security, facilities, isolation from and protection of the public, access control, and CCTV monitoring.

In the event that CP operations must be moved, plan for an alternate site capable of supporting the basic elements of operation. This will require adequate mirroring of the electronic infrastructure, and the means to switch over to the alternate systems, which may include wireless capabilities.

A location allowing the CP to have a direct view of the airside and the aircraft isolated parking position is desirable, and may be facilitated by the use of CCTV equipment. The CP location should be soundproof.

A mobile CP is a viable option at many airports, but requires allotments of support space and a coordinated communications infrastructure, possibly including wireless.

7.5.7.3 Space Needs

An ideal CP configuration consists of space sufficient to support the needs of the Crisis Management Team. A Crisis Management Team is generally composed of an operational group of key decision-makers, and may include other personnel, such as hostage negotiators or counter-terrorism experts. Designers and planners should refer to the requirements of the Airport Emergency Plan and the ASP to determine the optimum number of persons to be accommodated; information found in A/C 150/5200-31C, Airport Emergency Plan, can assist.

7.5.7.4 Other Considerations for CP, SOC, and EOC

- In some cases, the use of raised flooring is an option to provide for flexible installation of ducts and cable paths, and for additional equipment during an incident or a future reconfiguration of the room.
- Electrical power must be uninterrupted, which is accomplished by a dedicated UPS within the CP itself, or by being linked to a “no-break” power source or generator.
- Secure vehicular access to the CP should be considered.
- Sufficient controlled vehicular parking areas, preferably airside but in close proximity, should be provided for support vehicles (fire, off-airport mobile communications vehicles, etc.) and key CP vehicles.
- Consider the placement of an executive conference room adjacent to the CP for executive briefings and conferences.
- Provide space for kitchenette and rest rooms, and rest/sleep facilities for long term events.

7.5.8 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 assure the privacy of its users. See the National Transportation Safety Board’s family assistance documents.

7.5.9 Federal Inspection Service

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 air traffic.

Since FIS requirements are almost entirely related to international air service terminals, the subject is addressed at much greater length in Appendix D, International Aviation Security. In addition, there is extensive material provided by CBP that more fully specifies additional security design requirements for FIS space. Planners should consult with local CBP and other FIS representatives to ensure use of the most current version of standards, and to coordinate requirements with the CBP and other FIS agencies early in the design process. See also Appendix C of this document.[13]

7.5.10 Loading Dock and Delivery Areas

Loading docks and delivery areas are very active areas at airport terminals. Maintenance personnel, vendors and suppliers, delivery vehicles, service vehicles such as trash and recycling, and many others use this area constantly. 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. 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, concessionaires, 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.

Security strategies should allow efficient functioning of the area relative to the location, and access of the dock and the risk assessment at the particular airport. Access control of doors, personnel monitoring by airport delivery recipients with ID media, screening of delivered merchandise, and CCTV monitoring, 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 under-carriage, of all delivery vehicles approaching the terminal might be required, with consideration for 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. CCTV 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.

7.5.11 Cargo Facilities and Security Considerations

Generally, cargo facilities are subject to precisely the same physical security requirements for planning and design purposes as any other facility on the airport, although their procedural and operational differences often require some site-specific modifications or upgrades. Current regulations that require screening of all cargo that travels as belly freight in passenger aircraft are also likely to affect design alternatives for cargo carriers, freight forwarders, and other facilities where cargo arrives by truck and is accepted at loading docks.

[13] Additionally, PARAS 0002 Companion Guide to CBP's *Airport Technical Design Standards* is expected to be available in April 2017.

7.5.11.1 Overview of Air Cargo

The TSA is responsible for ensuring the security of all modes of transportation, including cargo placed aboard passenger and all-cargo aircraft. The implementation recommendations of the 9/11 Commission Act of 2007 specifically require 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, including secure areas of freight forwarder facilities, other cargo shippers 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 involving facilities where air cargo is sorted, screened, or loaded onto pallets or containers is necessary to ensure that security requirements are addressed.

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.

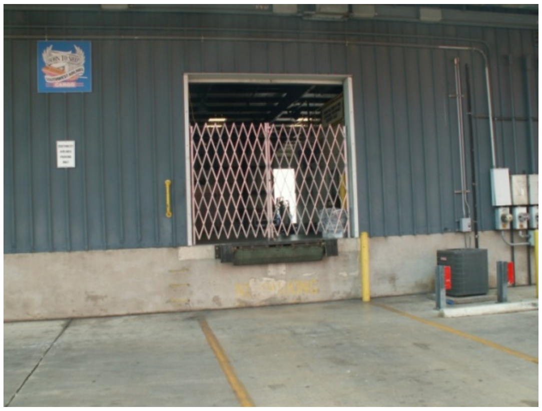
There are some basic physical security similarities that these types of facilities share when located on any airport property. These include the establishment and support of a perimeter around the facility, access control and credentialing protocols for employees, as well as lighting and CCTV surveillance of the facility.

7.5.11.2 The Cargo Facility Perimeter

The considerations for the establishment of a perimeter depend largely on the location of the facility. Access control and other security requirements may differ, depending on the operation's location with respect to the perimeter or as a part of a larger consolidated complex.

Considerations for an airside facility include the continuation and maintenance of a fence line that meets or exceeds the requirement of the airport operator's ASP.

Figure 7-1. Scissor Gate on Public Side of Building



Source: Jose Chavez

All authorized-personnel doors or gates that permit access to any airside portion of an airport, as well as airside-facing and landside-facing cargo doors, need the appropriate access controls as required in the ASP. Scissor gates, as shown in Figure 7-1, or other gates installed on the cargo doors facing the public side of the cargo facility permit ventilation and must be combined with the appropriate procedures to maintain the integrity of the airport perimeter. Appropriate lighting is also necessary around the perimeter of the facility as well as inside the facility.

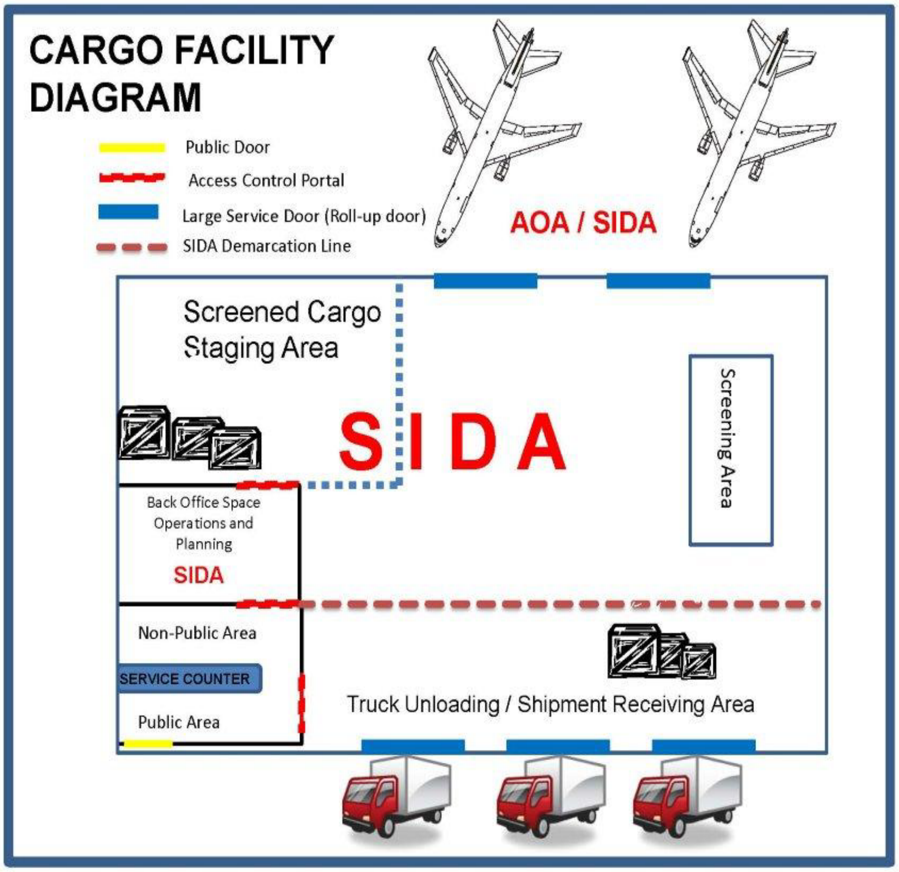
During the design process, planning should occur to minimize the possibility that the rooftop could provide access from the public side of the facility. Some measures include designing truck and vehicle parking areas far enough away from a building's façade as to make it impossible to gain access to the roof by climbing on to a truck or other vehicle's roof. Where possible, automobile parking should be separated from truck parking and located away from the building. Access ladders and doors leading to the roof of the facility, made necessary for the maintenance of HVAC and other mechanical systems, should be located away from public access or secured appropriately. Whenever possible, these roof access points should be located in an airport-controlled area of the facility.

7.5.11.3 Access Control to Operational Facilities

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 environment, 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 7-2, 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.

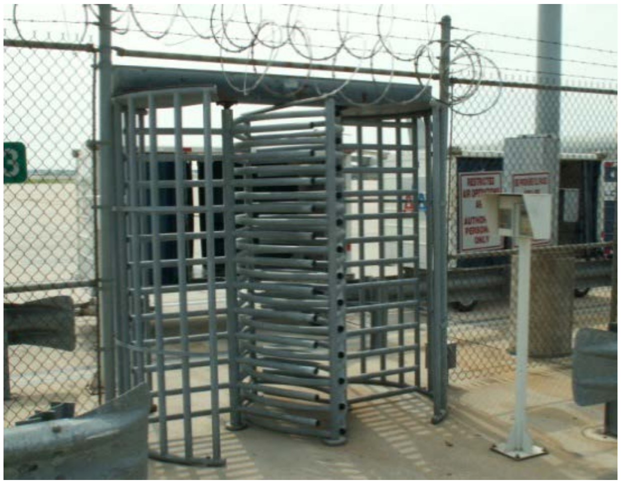
Figure 7-2. Cargo Facility Diagram



Source: Jose Chavez, TSA

Employee access control at a larger cargo facility may entail a more complex approach, including one-way gates. Larger facilities with a high number of employees would tend to use an electronic access control system, with card readers and the same ID media used by the airport operator, and incorporating alarm monitoring and LEO response.

Figure 7-3. One-Way Revolving Personnel Gate



Source: Jose Chavez

Public access to a facility should be limited to a counter area with direct landside access that allows for the transaction of any business, but prevents unauthorized access to such restricted areas as administrative offices, the ramp, cargo screening areas, and screened or unscreened cargo within the warehouse. Regardless of the type of access control system, the system should be scalable to allow for upgrades to access and monitoring control systems. One typical design feature is the establishment of a lobby and reception counter area. Whenever cargo is accepted from the public for shipment, access control points that are accessible only to appropriately badged employees must exist between the counter and any non-public area where cargo is inspected, sorted, and prepared for transport (see Figure 7-3).

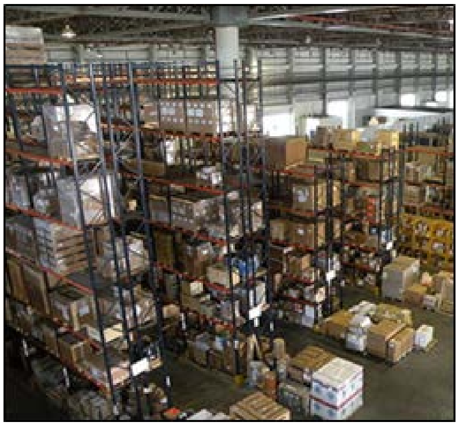
7.5.11.4 Cargo Facility Space Planning and Screening Process

Regardless of the type, size, or location of the facility at an airport, consideration for the flow of cargo through a facility should be part of the design plan. The flow of cargo, customers, and employees has an impact on the layout and the efficiency of the facility. Cargo handling and control drives the overall allocation of space for movement of shipments from receiving, to screening and cargo consolidation, and ultimately to aircraft loading. Consideration for space includes the storage of cargo that has not been screened, bulk pallet inspections, and secure cargo holding areas. The separation of public access areas within the facility from secured cargo areas needs to be determined; access to screened cargo must be limited only to authorized personnel.

Within a cargo facility, cargo should be segregated based on its position in the screening process. Certain cargo may arrive prescreened and ready for loading. This may require separate access doors to optimize cargo flows. It should be held with cargo that is received, screened, and palletized at the facility and is awaiting shipment. Both these segments should be segregated from cargo just received or undergoing the screening process. In the event that screening will take place in the cargo facility, additional space allocations should be provided for the breakdown, screening, and buildup of cargo pallets and containers. Cargo segregation may also include separating cargo destined for passenger carriers or all-cargo (freighter) carriers, known and unknown shipper cargo, or cargo being transported under a Customs bond. In designing the inside of the facility, planners and designers should give thought to how the screened cargo should be segregated.

In certain instances where cargo is transferring directly from one aircraft to another, a separate holding area may be required. In small facilities, a simple demarcation line, conspicuously painted on the ground, may suffice. In larger facilities, the screened cargo may need to be segregated by means of large cages built into the facility with access controls on the portals to prevent tampering. High vertical rack storage (see Figure 7-4) will require maneuvering space for tugs and forklifts, and possibly sight lines for high and low lighting and CCTV surveillance. In many new facilities, there is a trend toward common use, i.e., a single building operator for multiple tenants. In such instances the installation of a sophisticated material handling system may substantially alter the floor layouts and simplify the routing of cargo and its storage pending delivery to the aircraft or on the inbound side, to the consignees. Special accommodations may be necessary for high value, perishable goods or refrigeration requirements.

Figure 7-4. Cargo Facility with High Vertical and Wide Aisle Space



Source: Jose Chavez

7.5.11.5 Surveillance of the Cargo Facility, Employees and Processes

In designing both the inside and outside of the facility, planners should consider the need for CCTV surveillance for added security, deterrence, monitoring of processes, proof of regulatory compliance, and forensic evidence. Auto-dimming LED is now the preferred lighting for these environments. CCTV system requirements and design are covered in considerable detail in Section 12, Video Surveillance, Detection, and Distribution Systems of this document. Critical locations for CCTV coverage and appropriate lighting at a cargo facility include:

- The public side loading dock where large shipments of cargo are accepted
- The customer service counter where parcels are accepted from the public
- The area where cargo is screened
- The areas inside the facility where screened cargo is staged for shipment
- The ramp area on the non-public side of the facility
- All doors giving access to the airside (AOA/SIDA) of the airport
- Any portion of the building that abuts the airport's perimeter
- Public and employee parking areas

In large facilities such as the one pictured in Figure 7-4, CCTV monitoring of cargo and its screening process and storage presents challenges for the designer, including high vertical space with multiple narrow aisles and cargo-handling vehicle traffic, which require added consideration for the installation and use of lighting to provide proper surveillance of the facility. Lighting and CCTV must be considered jointly to support the type of CCTV system and lenses used. Light sources (e.g., mercury vapor, high and low pressure sodium vapor, metal halide, etc.) affect the quality of the images being observed and recorded by the CCTV system.

7.5.11.6 Access for Delivery/Distribution of Airport-Related Commercial Goods and Cargo

During airport design, it is important to consider areas where goods and services can enter or exit the airport. These goods include concessions-related items (food, beverage and retail items), airport business related items (paper, office supplies, and maintenance items), and trash removal. Additionally, some airports may run a third-party cargo handling facility as a non-aeronautical revenue source. In this case, such cargo could also fall into this category of items that need to be screened prior to entry into the SIDA/Secured Area.

In order to receive these goods with the highest levels of security, it is important that the location for this activity be considered early in the design process. In most cases, the most efficient process for receiving these goods is for the vendors to have direct access to the drop-off or pick-up location from a public (possibly restricted) roadway that does not require access to the AOA, SIDA, or Secured Area. Many of the goods will be destined for the terminal, so adjacency of the drop-off location to the terminal is also helpful. The drop-off area should provide loading dock facilities for trucks as large as tractor-trailers. The goods themselves need to be received in an area where they can be inspected and/or screened upon arrival. Ideally, provision of areas where the goods can be stored in the SIDA/Secured Area until they can be retrieved by the vendor for transport will provide flexibility and potential capital and operational cost savings.

Meeting the access requirements discussed above—adjacency to a public road, the airside, and the terminal—means that it is important to consider its location early in the design stage. The ideal site is likely at a nexus of the airside, landside, and terminal building. If a location can be identified that fulfills all of these requirements, delivery of commercial goods will have very limited need for vendors to enter the AOA, SIDA or Secured Area of the airport, leading to safety and security enhancements at the lowest possible operational cost. It will also minimize the need for goods to travel through the passenger security screening checkpoints, thus avoiding associated congestion and customer service impacts.

Delivery facilities required are:

- *Loading Dock:* Designed to accommodate the peak drop-off activity, normally early in the morning. The dock should accommodate deliveries by tractor-trailer trucks, step-vans, and required material handling equipment. The loading dock platform should be large enough to provide staging for off-loading of product during the receiving process, as well as adequate vehicle circulation. Good lighting for both the outside and inside of the loading dock is necessary. If airport policy requires coverage of the area with CCTV, the lighting levels both outside and inside should be adequate to ensure the effectiveness of the CCTV system. Lighting levels inside the loading dock must be adequate to clearly read package labels and any receiving equipment/system readouts as may be required to verify and inspect deliveries.
- *Security Processing Equipment:* Current TSA regulations require that products destined for SIDA, Secured, and Sterile Areas of the airport be inspected. Some airports may require some level of machine-screening capability, either now or in the future. It is important that adequate space be provided for the required inspection/screening process during peak receiving hours. Designers should consider what may be required in the future regarding screening, and incorporate the flexibility to scale the inspection process for potential future needs. Typically, this would require additional space, power, and IT capabilities.
- *Storage Areas:* At a minimum, secure storage for received goods needs to be provided in the receiving area so that products can be temporarily stored until delivery to consignees or further air shipment. The airport's receiving process and contracts with their concessionaires and possibly third-party cargo handlers determines how big these storage areas need to be. If the airport and its concessionaires have developed processes to support consolidated receiving of product, and so long as significantly sized long-term storage areas are not located throughout the terminal building, it is quite likely that the most space- and manpower-efficient solution for storage is to provide consolidated, long-term storage facilities in the receiving area. The storage would need to be sized to accommodate the peak demand for dry, refrigerated, perishable, frozen, and high value goods, segmented and secured for each concessionaire, in the SIDA or Secured Area of the terminal. Once the concessionaire retrieves their goods, they will need to follow the airport's security procedures to ensure that the product remains secure during its transit to their facilities. Depending on the airport's security policies, the need for a continuously secure path may also have a planning/design impact that should be considered. Also, if an airport elects to follow a consolidated receiving and storage philosophy, and in order for the airport to reap the productivity benefits of such a policy, it is important that only short-term storage areas be provided in other areas of the terminal adjacent to concessionaires. Otherwise, there is the possibility of facility over-sizing, and that may not be cost justifiable.
  - *Employee Support Areas:* Depending on the size of the receiving/storage area and availability of adjacent facilities, consider the need to incorporate restrooms, break rooms, communications, and other spaces in the design.
  - *Other Security Systems:* Based on the ASP, the designer of the consolidated receiving area needs to consider which of these systems are required to be incorporated in the design. These may include access control systems, possibly with biometric enhancements, CCTV systems, and passive surveillance systems.

Designers should reduce the number of delivery portals to sterile and secured/SIDA areas to the absolute minimum number possible based on the airport's physical configuration. The ultimate goal should be to consolidate all deliveries to a specific location or a reduced number of locations, increase ramp safety and security, and reduce inspection costs. Especially with respect to receiving operations, designers should consider that any processes or practices that can be standardized will produce both operational and cost benefits, as well as increased levels of safety and security.

7.6 Common Use Areas

During the planning and design process, consider the option of common use facilities for the airport and air carriers, e.g., Common Use Passenger Processing Systems (CUPPS).

Some airports now offer CUPPS, which can reduce the need for multiple security area separations and boundaries among users. This process involves ticketing, gate use, and bag claim functions. CUPPS follows normal procedures for handling passengers, and yet reduces costs to airlines while increasing use of an airport's capital assets—gates, ticket areas, and bag claim. CUPPS may result in a greater number of passengers handled, effectively reducing the need for an airline's territorial expansion, or enabling the airline to defer expansion to a later date. Inherent in a CUPPS is the airport operator's ownership of computers, cabling, loading bridges, bag belts, and the maintenance thereof.

7.7 Terminal Vulnerable Areas and Protection

Terminals are not isolated entities; they are part of a complex, integrated series of facilities that provide the basic and varied services of a modern airport. There are other areas outside the terminal where both terminal and overall airport security may be compromised.

Connections from the incoming utility services into the terminal complex are typically most vulnerable in the areas of power and communications. Transformers and switching gear, generating equipment, and transmission facilities are points of vulnerability for terminal facilities, and key connection points are sometimes located outside the perimeter. Planning and design should account for these elements and provide for their protection from several kinds of possible failure, including by intentional interference or natural disaster. Communication is also fundamental to terminal operations and security. Voice and data switching and transmission facilities should be planned and designed to be as secure and redundant as practicable to avoid disruption.

Utilities may cross the terminal perimeter through below-grade utility tunnels or ducts, which could provide surreptitious access to secure areas when they open into areas beyond the security controls. Planners should consider controls on such access points, including locking manhole covers.

Loading docks and delivery areas have been discussed in earlier sections in relation to access for daily airport operations. The security of these areas is a strategic necessity that should be developed in early planning.

The terminal also may have walkway or bridge connections to other terminals, hotels, parking structures, or other airport facilities and structures, including underground paths. Security strategies should be developed to control the movement of people through these connectors, and on the other surfaces of the connectors, such as roofs or interstitial spaces.

Many airports also provide people-moving systems that move persons within a terminal or from one terminal to another, whether underground, above ground, or on elevated railways. If exposed, these conveyance systems can also become points of significant vulnerability. The planning and design of these systems should consider not only terminal security, but where the conveyances cross through or above portions of the airside and landside.

7.8 Chemical and Biological Threats

Airport planners should be cognizant of the potential of chemical and biological (chem/bio) threats to their facilities. A chem/bio attack can be viewed as use of a weapon of mass destruction with significant economic impact. The development of appropriate facility and procedural responses to a potential chem/bio attack will provide an effective response to any of several types of chem/bio scenarios.

It is possible that the airport visitors, passengers, and staff could be threatened by a non-terrorist accidental release or volatile inhalation of hazardous industrial chemicals, like chlorine or ammonia. This release could happen off airport property but require appropriate facility HVAC management and that personnel shelter in place.

The public area may be exposed to a perceived or actual noxious chemical release—perhaps an abandoned leaking pepper spray container or an item confiscated at a checkpoint—that will require assessment, limited evacuation, mitigation, and removal. An actual chem/bio agent released in the public area might also require decontamination of people and facilities, as well as appropriate medical treatment. Preparation and appropriate responses to all of these scenarios will minimize any injury to passengers and staff, and return the terminal to operation in a timely fashion.

Historically, terrorist-placed devices have been small and of limited effectiveness, but their publicity, economic impact, and facility disruption have been significant. Facilities can be contaminated and out of economic production for a year or more. It is conceivable that a chem/bio attack could be launched against any element of an airport to disrupt the overall operation; however, the passenger terminal is seen as the most likely target.

Preparation for the renovation or building of a new terminal or airport facility should be planned to accomplish two objectives:

- To deter attacks through HVAC-system physical security
- To mitigate the consequences of an attack through passive protection and active response measures

In accomplishing the first objective, the planner should recognize that protecting a facility against a chemical or biological agent introduced into the HVAC system could involve substantial effort and cost. The first step is to identify those groups that should be involved in the ConOps for the planning effort: security personnel, HVAC engineers, public safety representatives, maintenance crews, and airport management. Many of these entities will already be part of the planning process for building development.

The starting point for facility protection is gaining an understanding of the threat:

- What are characteristics of chem/bio agents?
- What is the scope of the threat?
- What are plausible release devices and attack scenarios?

Once the threat is understood, the next step is an assessment of the vulnerability of existing systems. What physical security measures, airflow characteristics, and response capabilities are already in place, and how might they deter and/or mitigate the consequences of an attack?

The likelihood and/or severity of an attack can be affected by fixed physical characteristics such as HVAC physical security; by technical capabilities such as the ability to manipulate HVAC systems remotely; and by personnel alertness, training, and coordination. Information from several airport departments is typically needed to successfully complete an assessment.

For existing facilities, the initial assessment should be an overview exercise, with the assessor consulting with subject matter experts, and perhaps brief orientation tours of selected areas of the facility. A more in-depth assessment might involve physical examination and/or testing of relevant systems, including a team of experts and possibly external consultants. Once the assessment is complete, the next step is facility hardening. What system upgrades and responses would better deter and/or mitigate the consequences of an attack?

The facility hardening phase focuses on three elements:

- Attack prevention through HVAC-system physical security
- Attack mitigation by passive protection using airflow control, i.e., protection measures that will deter and/or mitigate the consequences of an attack even without knowledge of the attack
- Attack mitigation through active response, i.e., actions to be taken in the event that a suspected attack is discovered—these might include evacuation, triage, quarantine facilities, detoxification facilities, medical mutual aid response capabilities, and screening of vehicles, among others

One consideration is the use of chemical and biological detection systems for building protection. There are two types of systems in operational use. Chemical sensors that can detect some classes of volatile chemical agents are deployed operationally to provide early warning of chemical releases, and to enable rapid and effective facility responses. Such a system has been in operation in the Washington, D.C. Metrorail stations for several years.

As of the publication of this document, real-time bio-detection equipment is not sufficiently mature for operational systems. However, the DHS BioWatch Program is deploying aerosol collectors in facilities across the country, including in airports, from which samples are taken periodically to laboratories for analysis and detection of bio-agents. Bio-detection with such a system does not enable real time responses, but does allow exposed individuals to be identified within a few days and treated before they become ill, significantly improving their chances of survival. Such post-attack detection also allows contaminated facilities to be identified and isolated, preventing additional exposures and additional spreading of contamination.

Airport operators should explore the potential uses of available detection technologies during planning and design; additional guidance on threat awareness, bio-surveillance, detection/diagnostics and response/recovery is available from DHS at https://www.dhs.gov/science-and-technology/st-cbd.

For a fuller discussion of chem/bio guidance, airport architects, security and emergency planners, and others are encouraged to obtain a copy of the airport chem/bio protection document, *Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism* developed by Sandia National Laboratories and Lawrence Berkeley National Laboratory under DHS’s PROACT (Protective and Responsive Options for Airport Counter-Terrorism) Program. The report can aid airport planners in defending their facilities against chemical and biological attack, given the technologies and capabilities available. With the report, airport planners should gain an understanding of the important issues for chem/bio preparedness, and should be able to assess the status of their airport to determine whether to bring in consultant expertise, and to target the most effective upgrades for their facilities.

7.9 Checklists

Terminal Security Architecture Checklist

□ Design to be flexible; technology and regulations change

□ Coordinate access points, minimize crossing security boundaries

□ Planning and Design Considerations
- Physical security-level boundaries
- Prevent items being passed through/over physical boundaries
- Deter public access to nonpublic areas

□ Bomb/Blast Analysis
- Critical in early design
- Review periodically

□ Limited 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

□ Minimum Number of Security Portals
- Minimize for cost and security
- Reduces cost of personnel screening
- Remain flexible for future expansion

□ Space/Infrastructure for Added Measures
- Allows growth, minimal impact
- Reduces installation costs
- Reduces time needed for expansions

□ Consider space/accommodations for:
- Temporary/additional SSCPs
- Delivery and personnel screening
- Expansion to primary SSCP

Terminal Area Users and Infrastructure

□ Meet with all relevant airport users to determine user requirements in ConOps

□ Consider both horizontal and vertical circulation patterns

□ Security support for utility infrastructure (power, data, communications)

□ New construction vs. alterations—both require the same attention to security

Sterile Areas Checklist

□ Area between the security screening checkpoint and door to aircraft

□ Objective: passenger containment, prevent access to contraband

- □ Number of access portals limited to minimum operational necessity
- □ Comply with local fire/life safety codes, ADA
  - ▪ Prevent articles from being passed from public to Sterile or Secured Areas
  - ▪ Consider paths of access in restrooms, airline lounges, kitchens, plumbing chases, air vents, drains, trash chutes, utility tunnels or other channels
  - ▪ Consider multiple access needs of airport, airline, maintenance, tenant and concession staff
- □ Emergency response routes for off-airport response, ARFF/fire, EMS
- □ Concessions access for delivery requirements inside security
- □ Built-in security-friendly fixtures (railings, pillars, benches, ashtrays, trash cans)

Public Areas Checklist

- □ Public lobby areas (ticketing, bag claim, rental car)
  - ▪ Limit number of access points
  - ▪ Monitor portals and conveyors
  - ▪ Furnishings—avoid concealment
  - ▪ Seek structural advice on minimizing blast effects
  - ▪ Ticketing lobby
    - ▸ Minimal seating to reduce congestion
    - ▸ International operators have extended security measures
- □ Public emergency exits
  - ▪ Coordinate code requirements with fire marshal
  - ▪ Avoid moving from lower to higher security
  - ▪ Consider push-type bars with 15–30 second delays
- □ Concessions areas
  - ▪ Consider temporary move during heightened security
  - ▪ Short delivery routes minimize crossing security boundaries
  - ▪ Consider type of concession: storage, high-value, ATMs
- □ Prevent public access to the airside via connecting elevators, stairwells
- □ Signage for FIS
- □ Eliminate public area lockers
- □ Unclaimed luggage area—coordinate with EOD/LEO access
- □ VIP lounges/hospitality suites
- □ Observation decks discouraged

Nonpublic Areas Checklist

- □ Service corridors, stairwells and vertical circulation
  - ▪ Minimize access points, do not cross secure boundaries
  - ▪ Tenant areas grouped in common service corridor
  - ▪ Needs of emergency/LEO
- □ Airport personnel offices
  - ▪ Minimize crossing security boundaries
  - ▪ Consider satellite police sub-stations, ID or first aid offices
- □ Tenant spaces

    - Some may require tie to airport access control and alarm system
    - Consider tenant money-handling, overnight operations

- □ Law enforcement and public safety areas
    - Public safety or police offices
        - Office space in the terminal—consider communications links
        - Protected with ballistic materials, bollards, etc.
        - Public access to administrative, ID offices, lost and found, training rooms, EMT
    - Law enforcement parking—direct landside to SIDA access
    - Remote law enforcement/public safety posts/areas, substations, and outdoor shelters
- □ Dogs/K-9 teams
    - Specify non-critical K-9 area
    - Rule of thumb: 4-foot by 8-foot indoor pen attached to outdoor fenced exercise run
    - Plumbing and drainage; epoxy coated floor for cleaning
    - Fresh air circulation, dry, no mildew or dampness
    - Secured, isolated from casual public contact
    - Isolation from noise and odor sources, especially jet fuel fumes
    - Secured storage for explosives test and training items
- □ Security Operations Center (SOC)
    - Multiple communications needs for police, fire, rescue, airport operations, crash/hijack alert, off-airport emergency assistance
    - Locate close to the Airport Emergency CP
    - Central cabling interconnections, reasonable cable lengths
    - Rear access to console for maintenance
    - Space requirements for all LEO functions in SOC
    - Plan alternate site for basic operation.
    - Direct view of the airside and isolated parking
    - Other considerations
        - Raised flooring installation of ducts and cable paths
        - CP electrical power UPS
        - Access for support/CP vehicles
        - Space for kitchen, rest areas
- □ Family assistance center—access-controlled space
- □ Loading dock and delivery areas
    - Access control and identification media
    - Package screening
    - CCTV
    - FIS areas (coordinate with CBP)

Terminal Vulnerable Areas and Protection Checklist

- □ Complex/multi-use function of public terminals contains the broadest range of vulnerable areas
- □ Each airport is unique and should be evaluated for unique or increased vulnerabilities
- □ Terminal Vulnerable Areas
    - Connections from the terminal to utility services in power and communications
    - Hotels, parking structures or other on-site or adjacent public facilities and structures
    - Loading docks and delivery areas
    - Locations for person or object concealment

- People moving systems, if exposed, including underground and elevated rail
- Primary transformers, switching gear, and UPS
- Secondary generating equipment and transmission facilities
- Utility tunnels or ducts entering a terminal below grade
- Voice and data switching and transmission facilities
- Walkway or bridge connections to other terminals

Cargo Facility Checklist

□ Cargo Facility's Perimeter
- Fence/boundary consistent with ASP
- Access control and monitoring, lighting
- Public access limited
- Scalable to allow for upgrades

□ Space Planning and Screening
- Efficient flow-through of cargo is paramount
- Secure storage space for unscreened cargo
- Cargo segregation based on screening progress
- High vertical racks require vehicle maneuvering space
- Secure storage for high value, perishable goods

□ Surveillance—Critical CCTV 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

□ Airport-Tenant Related Commercial Cargo
- Concessions, businesses, trash removal
- Direct access to the drop-off/pick-up location
- Provide loading dock facilities for trucks as large as tractor-trailers
- Receiving area for inspection/screening
- Adjacency to a public road, the airside, and the terminal
- Minimize need for travel through security screening checkpoints

□ Airport-Tenant facilities required
- Loading dock to accommodate peak drop-off activity
- Provide staging space for off-loading
- Adequate vehicle circulation
- Good lighting for CCTV, loading dock
- Security processing equipment
- Scalability for future screening requirements
- Additional storage space, power, and IT capabilities

SECTION 8: BAGGAGE HANDLING SYSTEM

8.1 Introduction

This section is a summary of the *Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems (CBISs)* prepared by the TSA. To provide structured guidance on industry best practices, and to convey TSA requirements for CBISs, the PGDS was developed as an industry reference on how to develop cost-effective screening solutions that ensure the needs of all stakeholders are addressed.

The main objective of this section is to outline what airport operators need to be aware of before planning, designing, and implementing CBISs. Before beginning the planning process, it is essential that the details in the PGDS that apply to the project are reviewed and understood.

8.2 CBIS Overview

There are three broad categories of CBIS: stand-alone (using either Explosives Trace Detection [ETD] or Explosives Detection Systems [EDS]), mini in-line, and full inline.

A stand-alone CBIS is a decentralized system that is not integrated into the outbound baggage handling system (BHS), and therefore has a much lower screening throughput. A mini in-line CBIS contains one EDS unit to screen baggage, which flows from a bank of ticket counters on a single take-away conveyor that is integrated with the EDS. A full in-line CBIS is integrated into the baggage handling system, consolidating baggage flows from multiple inputs into a centralized matrix of EDS screening units. The planning and design of in-line CBISs is the most complex and therefore the focus of this preliminary guidance, as well as the PGDS.

An in-line CBIS is defined to include from the point of bag induction, through the EDS screening area, to the point where bags are delivered to the airlines' outbound sortation or make-up system.

As shown on Figure 8-1, the screening process occurs between the point where bags are loaded onto induction belts—usually at the airline check-in counters (input lines)—and the point where they are delivered to the airlines' outbound sortation or make-up system.

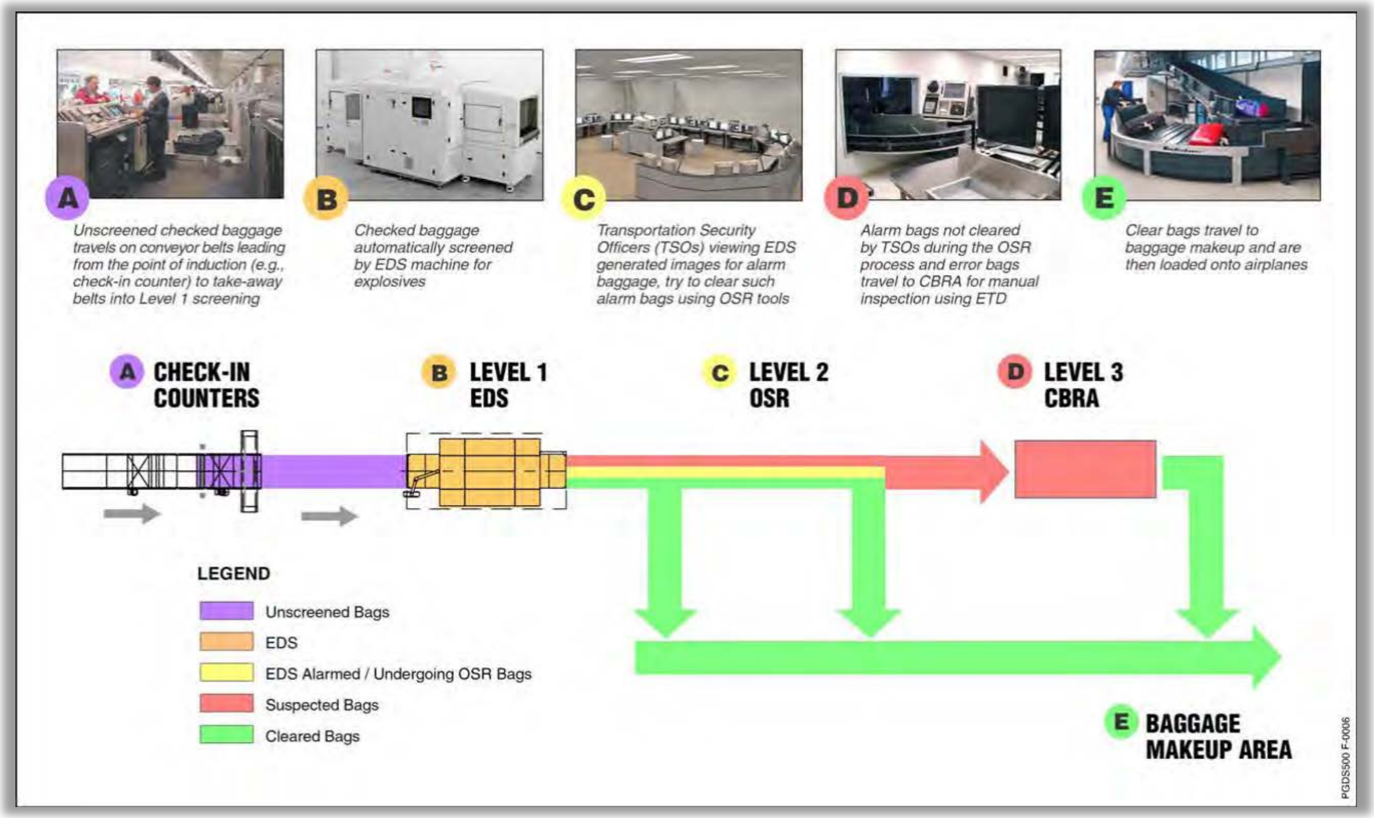
The process involves the following three screening levels:

Level 1 screening is performed with EDS equipment. All bags that can physically fit in an EDS unit are directed to Level 1 screening and scanned using an EDS. All bags that automatically alarm at Level 1 are subject to Level 2 screening. Bags that cannot effectively fit within an EDS unit are either deemed to be "out of gauge" (OOG) by measurement devices within the BHS, or manually determined to be "oversize" prior to input at the induction point, and transported directly to Level 3 screening, bypassing the EDS matrix.

During **Level 2 screening**, TSA personnel view alarmed bag images captured during the Level 1 EDS scan, and adjudicate alarmed objects in the bag to provide a Clear or Alarm designation for the bag. This process is referred to as On Screen Resolution (OSR) which, for in-line systems, allows the continuous flow of bags through the system until a decision is made. Although OSR typically occurs in a remote screening area, it could occur locally at the individual EDS, but only in a mini in-line or stand-alone configuration. All bags that cannot be resolved at Level 2 (e.g., Time Out Bags) and all bags that cannot be directed to Level 1 because of size restrictions are automatically transported to Level 3 screening.

Level 3 screening is performed manually by Transportation Security Officers (TSOs) in a Checked Baggage Resolution Area (CBRA). This involves opening the bag and the use of ETD technology. For those bags whose images were captured during Level 1 screening, the TSO may use a directed search protocol in lieu of a full bag search. Once a bag is cleared, it is manually returned to the BHS and transported to outbound make-up. Bags that do not pass Level 3 screening (typically, a small percentage of total bags) are either resolved or disposed of per the current TSA checked baggage SOP, which typically involves a local law enforcement officer.

Figure 8-1. Overview of an In-Line Checked Baggage Inspection System


A
Unscreened checked baggage travels on conveyor belts leading from the point of induction (e.g., check-in counter) to take-away belts into Level 1 screening
B
Checked baggage automatically screened by EDS machine for explosives
C
Transportation Security Officers (TSOs) viewing EDS generated images for alarm baggage, try to clear such alarm bags using OSR tools
D
Alarm bags not cleared by TSOs during the OSR process and error bags travel to CBRA for manual inspection using ETD
E
Clear bags travel to baggage makeup and are then loaded onto airplanes
A CHECK-IN COUNTERS
B LEVEL 1 EDS
C LEVEL 2 OSR
D LEVEL 3 CBRA
E BAGGAGE MAKEUP AREA
LEGEND
Unscreened Bags
EDS
EDS Alarmed / Undergoing OSR Bags
Suspected Bags
Cleared Bags
PGDS500 F-0006

Source: TSA

8.3 Federal Funding Options for CBIS Design and Construction

The TSA is responsible for the deployment and installation of EDS equipment at airports across the nation. The Checked Baggage Technology Division (CBTD) is responsible for the identification of requirements through its Planning Branch, and for procurement of approved and available screening equipment.

Currently, the TSA offers two types of federal funding support to project sponsors:

- Design Other Transaction Agreements (OTAs)—Funding support for the design phases of a CBIS project
- Construction OTAs—Funding support for facility modifications during construction

Compliance with portions of the PGDS is mandatory. The latest version of the PGDS with which the CBIS must comply contains both requirements and best practices; the latter are not required. The latest version is confirmed by the TSA during the early stages of the design process, and further validated in the funding OTA or MOU for non-TSA funded projects.

8.3.1 Design OTAs

In order to increase TSA's involvement in the development of CBIS designs, with the resulting benefit of more efficient, cost-effective, and streamlined screening systems, the Electronic Baggage Screening Program (EBSP) will conduct targeted outreach efforts to strategic priority airports. A major tool in this outreach effort will be the Two-Phase OTA process. The Two-Phase funding process will provide an OTA to selected airports to support the development of a CBIS design (the "Design OTA"). Following the development of the design and the approval of a complete funding application package, EBSP may then enter into a second OTA with the airport operator for construction costs associated with the facility modification project (the "Construction OTA"), subject to the availability of funds.

Prior to execution of a Design OTA, EBSP will provide rule-of-thumb guidance on design costs to TSA for use in negotiating Design OTAs. TSA will provide the airport operator with optimal systems specifications, including information on equipment counts and the type of system selected. This information will serve as a starting point for the alternatives analysis to be performed by the airport. Airport operators will be asked to submit a notional schedule for the design effort to support EBSP's planning efforts.

8.3.2 Construction OTAs

Project sponsors applying for facility modification funding must obtain TSA approval of the Basis of Design Report to be eligible for facility modification funding. TSA will typically conduct a cost validation once bids are received in order to confirm the amount of the construction OTA.

The In-Line Funding Support Application Form, as part of the funding application process, is the vehicle through which TSA invites communication from project sponsors regarding project needs and funding requests. This process allows for proper tracking and handling of funding requests and subsequent communications between TSA and the airport.

Project sponsors are strongly encouraged to work with local TSA and headquarters TSA via Regional Deployment Coordinators as early as possible when EDS projects are being considered and conceptually planned. Early notification assists TSA in justifying federal funding for the CBTD.

8.4 Principles for CBIS Planning and Design

The objective of a CBIS project is to identify, design, and implement an appropriately sized, functional, and cost-effective baggage screening system. When planning a CBIS, project, sponsors should consider the following key principles:

- Achieve the lowest-cost solution. Achieving the lowest-cost solution requires:
    - Maintaining sufficient infrastructure flexibility and adaptability of design alternatives to accommodate future screening technologies still under development
    - Considering a wide range of alternatives rather than relying on a preconceived notion regarding which system would be best suited for a particular airport/terminal

  - Assessing the 20-year life-cycle costs of different alternatives, so that the ongoing costs of operating and maintaining these systems are appropriately balanced with the upfront capital costs.

- Follow design standards and BHS industry best practices. Design standards should be considered throughout the planning and design process and should be met during implementation via system testing but also during planning and design.
- Understand the complexity of in-line baggage screening systems, especially those with high levels of automation. Many different technologies for conveyance, tracking, and screening must all work together seamlessly to achieve an effective, efficient and reliable CBIS.
- Appropriately estimate demand and equipment requirements. The approach used to estimate demand and equipment needs for the initial system has a major effect on project costs. The PGDS provides a recommended approach to estimate demand and equipment needs, and clarifies the design year for various components of the CBIS—e.g., for screening equipment quantity, the design year is five years beyond the date of beneficial use (DBU+5). The level of upfront investment to accommodate demand beyond the date of beneficial use plus five years should be assessed using a 20-year life-cycle cost analysis.
- Consider how the CBIS will operate during contingency operations. The best approach for providing redundancy and establishing contingency operations will vary significantly depending on local conditions. In general, low-cost opportunities to “share” capacity across screening zones should be pursued before capacity is added to a specific zone. Regardless of the redundancies built into a particular system, a contingency plan must be developed with the consensus of key stakeholders, including airport and airline personnel, which defines how the CBIS will operate when screening equipment is unavailable, demand exceeds capacity, or a catastrophic system failure occurs. Note that TSA does not fund redundancy of systems, other than a “redundant” EDS (n+1) to account for EDS calibration cycles during peak times. A guide to contingency planning is provided in the PGDS.
- Provide flexibility in CBIS designs and facilities. Building in flexibility from the outset to accommodate future upgraded security technologies will keep future upgrade costs to a minimum while maximizing both current and future EDS performance. Given the rapidly changing nature of screening technologies and the threats facing the aviation system, flexible system design is crucial for successful implementation.
- Involve all relevant stakeholders. Stakeholder involvement is the key to successful and cost-effective CBIS implementation. This involvement needs to occur at both the industry/federal government level and the local/airport level.
- Understand reimbursable and non-reimbursable costs. It may be prudent to gain a good understanding of allowable costs associated with CBIS when seeking TSA funding.

8.5 Roles and Responsibilities

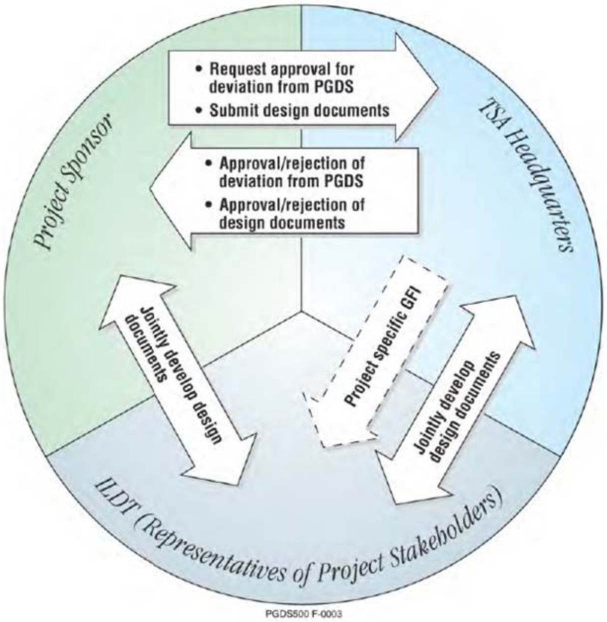
The following paragraphs summarize the roles and responsibilities involved in planning, design, and implementation of a CBIS. Figure 8-2, below, diagrams the described process.

- Project stakeholders should be periodically briefed on the progress of the planning and design effort. The stakeholder list should be customized to reflect the relevant stakeholders at the specific airport, and is anticipated to include the following primary functions:

  - Airport—Engineering, operations, IT, maintenance, planning and design, project management, and others as appropriate
  - Airline(s)—Headquarters, operations, corporate real estate, IT, maintenance, engineering, planning, security technology officer(s), station manager(s), and others as appropriate
  - TSA—FSD, Regional Deployment Manager, occupational health and safety representative and/or other technical representatives designated by the FSD, and a design review team from TSA Headquarters (TSA HQ)
  - Additional stakeholders—Local law enforcement and EDS equipment providers and manufacturers

- Integrated local design team (ILDT)—As part of the design process, an ILDT that includes representatives of some or all of the above-mentioned stakeholders should be formed. In addition, the ILDT should include a professional planning and design team that comprises architects, engineers, planners, CBIS designers, cost estimators, and project managers. The design team is also likely to include specialty consultants, such as simulation analysts and landscape architects, on an as needed basis. The ILDT is responsible for the development of alternative screening concepts, evaluation of those concepts, and generation of design drawings/submittals. In addition, the ILDT is responsible for the assessment of specific local conditions and standards affecting the CBIS design.
- Project sponsor—The project sponsor is assumed to be an airport owner/operator or an airline (if the system is for an airline-owned terminal). The project sponsor is responsible for initiation and execution of CBIS planning and design, formation of the ILDT, selection of a professional planning and design team, application for TSA or other funding, initiation, and execution of construction, as well as testing and commissioning of the CBIS, and operation and maintenance of the BHS portion of the CBIS.
- TSA HQ—Representatives from TSA HQ are responsible for reviewing and approving/rejecting design submittals. TSA will determine funding eligibility and prioritization, as well as assess issues related to occupational safety, health, and the environment. In addition, TSA will determine and provide the specific EDS equipment type to be used and schedule the testing and commissioning of the equipment.

Figure 8-2. Diagram of Interactions between ILDT and TSA HQ


Project Sponsor
TSA Headquarters
ILDT (Representatives of Project Stakeholders)
• Request approval for deviation from PGDS
• Submit design documents
• Approval/rejection of deviation from PGDS
• Approval/rejection of design documents
Jointly develop design documents
Project specific GFI
Jointly develop design documents
PGDS500 F-0003

Source: TSA

8.6 CBIS and Screening System Types

Planners and designers should consider several alternative solutions during the early design process. These range from highly integrated, highly automated, and low labor-intensive systems to low-automation and high labor-intensive systems (e.g., stand-alone EDS and ETD CBIS types). Figure 8-3 shows examples of CBIS types.

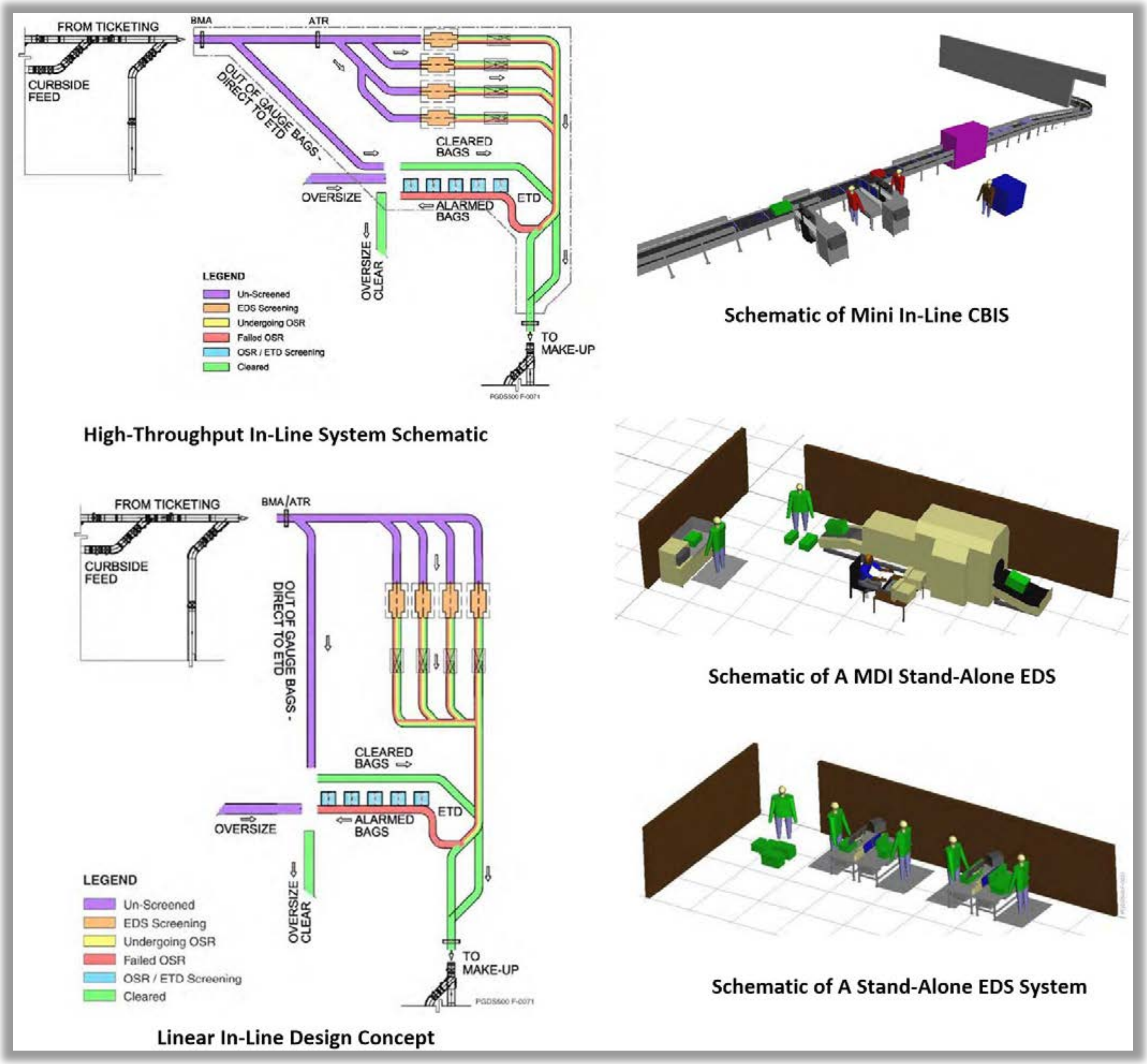
8.6.1 System Type 1: In-Line CBIS

In-line systems are assumed to have a very high level of integration and a sophisticated in-line conveyor infrastructure, providing sufficient queuing capacity and OSR circulation time while maintaining high throughput and accurate bag tracking. These systems are assumed to have multiplexed EDS technology (i.e., the capability of linking multiple EDS machines with multiple viewing stations), centralized control room(s), OSR capability, multiple baggage inputs, and CBRAs. Typically, these systems require automated baggage sortation.

The high-speed and medium-speed EDS machines used in this system type are intended to provide solutions for airports that require fully automated in-line systems designed to handle very high peak baggage screening demand. High-speed EDS machines are estimated to achieve at least a throughput of 900 bags per hour (bph) with a low false alarm rate, but none have been qualified for TSA purchase as of the publication of PGDS version 5.0. Medium-speed EDS machines must achieve throughputs of 400 bph or more per the TSA Procurement Specification. Throughputs for all qualified equipment approved for use in CBISs can be found in the PGDS.

Also, these machines are expected to have improved image quality and better OSR operator tools (such as high resolution 3-dimensional images of alarmed bags and alarmed objects, as well as density stripping tools). These OSR tools should enable operators to achieve higher clear rates.

Figure 8-3. Checked Baggage Inspection System Diagrams



High-Throughput In-Line System Schematic

Schematic of Mini In-Line CBIS

Schematic of A MDI Stand-Alone EDS

Schematic of A Stand-Alone EDS System

Linear In-Line Design Concept

Source: TSA

8.6.2 System Type 2: Mini In-Line CBIS

A mini in-line system would typically incorporate a simpler conveyor design and require a smaller footprint. These systems can be located on a take-away belt closer to airline ticket counters or baggage make-up devices, which can help reduce travel time and the likelihood of improper baggage sortation. A mini in-line system would include a single EDS machine to minimize system integration costs; however, airports may have multiple mini in-line systems to accommodate different airlines and/or bag rooms.

It should also be noted that screening systems placed close to ticket counters (and therefore with minimal conveyor distance leading to the EDS input) can be susceptible to dieback situations where bags can quickly accumulate on the conveyors back into the check in ticket counters. Where bag demand generated by self-service kiosks or other expedited check-in processes creates volume at a faster rate than traditional check-in methods, dieback can quickly occur because there is minimal queuing capacity on the conveyor system. Special consideration is required to anticipate ticket counter configurations and baggage delivery rates (including the variable nature of those rates) as part of the planning and design processes for these systems.

Since one of the objectives of a mini in-line CBIS is to minimize operational costs, redundant EDS are not supported by the TSA. Instead, redundancy will be achieved with other adjacent systems that could be used during a short–term failure of an EDS. During the design review process, the ILDT will be required to develop proper contingency plans for long-term failures that may occur to the EDS and/or conveyor system. Other redundancy or contingency solutions may incorporate additional inspection tables, automatic diverters, and/or OOG lines.

Because of the decentralized nature of these systems, staff and equipment needs would generally be higher than for centralized systems (such as in-line systems using high-volume or medium-volume EDS); however, upfront capital costs would be significantly lower. The mini in-line system is an option to reduce upfront capital costs where no economic justification exists to design and implement a full in-line system. Various mini in-line system configurations using different combinations of staffing levels and quantities of queue conveyors between the EDS exit and the baggage removal point are provided in the PGDS.

8.6.3 System Type 3: Stand-Alone EDS

In small airports, or in specific zones with low baggage volumes at larger airports, stand-alone EDS may be the most cost-effective option. A stand-alone EDS operates in a manner similar to lobby screening installed today at many Category X and Category I airports. However, where possible, stand-alone equipment should be installed in baggage make-up areas or other appropriate locations to reduce lobby congestion. This CBIS type is relatively labor intensive, but minimal capital investment is required to install the system and support the operation. It should be noted that no redundant stand-alone machines will be provided by TSA. A stand-alone system option would significantly reduce upfront capital costs by using currently available EDS machines with throughputs of at least 100 bags per hour in locations where no economic justification exists to design and implement an in-line system.

8.6.4 System Type 4: Stand-Alone ETD Systems

ETD equipment is currently used for primary screening (as an alternative to EDS screening, and as a means to screen OOG, oversized, fragile, and other baggage that cannot be screened using EDS), and for resolution of EDS alarms.

8.6.4.1 Primary Screening

Stand-alone ETD equipment can currently be used for 100 percent checked baggage screening in lobbies, baggage make-up areas, or other appropriate locations.

As ETD screening is the most labor-intensive screening method and has the lowest throughput compared with all other screening methods, ETD primary screening is typically only appropriate in lieu of EDS screening at airport zones with low baggage volumes.

8.6.4.2 EDS Alarm Resolution

ETD equipment is used as the primary method of screening bags when no EDS is present. ETD equipment is also used to screen EDS-alarmed bags that have not been cleared by operators using an OSR protocol (based on viewing bag images). This method is referred to as the Directed Search Screening Method, and is focused on identifying and locating objects within baggage that have triggered EDS alarms. Detailed information on current EDS and ETD equipment models is provided in the PGDS. This includes information regarding:

- Spatial dimensions
- False alarm rates and OSR clear rates (considered to be Sensitive Security Information available via request to TSA)
- Environmental operating envelope
- Weight and floor loading
- Procurement category
- Throughput rates
- Maximum bag size allowed and average percent OOG
- Expected life span
- Current procurement status (whether the machine is in development, certified but not yet available for procurement, or available for procurement)

8.7 Other Baggage Conveying System Types

The previous discussions have assumed the traditional “friction belt on slider bed” technology, but there are other types of baggage systems that utilize other means to accomplish the same goals. Individual Carrier Systems (ICS) are examples of alternate technologies for transporting baggage, and are often seen as destination-coded vehicles, tote-transport systems, etc.

An ICS-based CBIS design concept typically uses individual totes/trays/bins to carry baggage through a transport and sortation system, which allows for the distribution of bags to the EDS machines as well as to the CBRA, and if so designed, for the automated sortation of bags to multiple make-up devices. ICSs typically consist of a closed-loop conveyor system on which special-purpose totes (each accommodating a single bag and possessing a unique RFID tag) are transported to the EDS. In this type of system, the bag remains in the tote throughout the screening and sortation processes. Alarmed baggage is transported to the CBRA (in the tote) while cleared baggage is conveyed to the sortation system. The ICS concept is presented to provide planners with a broad range of potential CBIS concepts for consideration during the pre-design phase.

A key consideration in this type of design is that once loaded into the ICS, the bag must remain associated with that carrier throughout the screening process. Upon arrival into the CBRA, the bag cannot be unloaded/removed from the tote/tray/bin until an operator is available to screen the bag. Once the bag is removed from the tote/tray/bin by sliding the bag (lifting should not be required), the tote/tray/bin must remain at that location until the bag has been screened and loaded back into the same tote/tray/bin to maintain positive tracking.

Considering the complexity of this type of system, an ICS is most likely suitable for a large installation of a complete baggage system in a new or extensively renovated terminal, for a major airline hub operation, or for a large terminal with multiple airlines sharing a common EDS screening facility. It is most beneficial in a centralized screening operational design, where EDS and CBRA staff can be minimized without compromising time in-system constraints.

8.8 Development and Evaluation of Alternatives

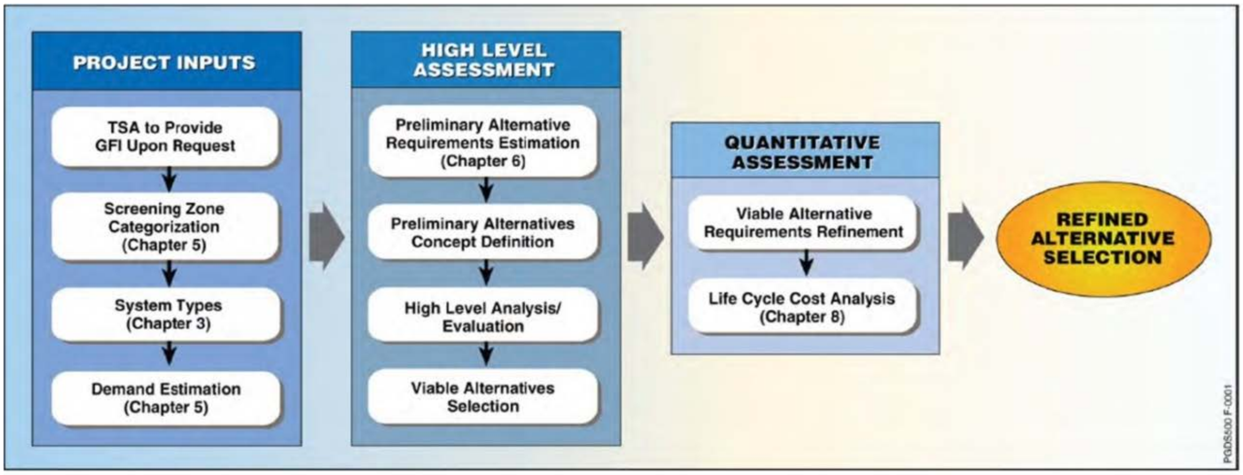
Planners should develop screening alternatives that account for the following:

- Airport Spatial Data — Terminal configurations, airline assignments, and architectural constraints
- CBIS Capacity Data — Data related to the type of screening systems and screening equipment
- Baggage Screening Demand Data — Factors affecting current and future baggage flow into the CBIS, such as existing infrastructure including ticket counter and curbside check-in positions, numbers of gates, and runway capacities
- Cost Data —Equipment, infrastructure, O&M, and staffing costs

Planners should develop alternatives based on the conditions at the specific airport. An initial high-level assessment should be conducted to identify spatially and operationally feasible alternatives based on forecasted demand. Subsequently, these alternatives will be evaluated on the basis of a 20-year life-cycle cost analysis for implementing, maintaining, and replacing the screening system. The lowest-cost alternative(s) that provides adequate screening solutions for the particular airport or terminal in question shall be selected as the preferred alternative(s).

Figure 8-4 summarizes the alternatives development and evaluation process to be carried out during the pre-design and schematic phases.

Figure 8-4. Pre-Design Phase Alternatives Development and Evaluation


PROJECT INPUTS
TSA to Provide GFI Upon Request
Screening Zone Categorization (Chapter 5)
System Types (Chapter 3)
Demand Estimation (Chapter 5)
HIGH LEVEL ASSESSMENT
Preliminary Alternative Requirements Estimation (Chapter 6)
Preliminary Alternatives Concept Definition
High Level Analysis/ Evaluation
Viable Alternatives Selection
QUANTITATIVE ASSESSMENT
Viable Alternative Requirements Refinement
Life Cycle Cost Analysis (Chapter 8)
REFINED ALTERNATIVE SELECTION
PGDS500 F-0001

Source: TSA PGDS

Planners should refer to the PGDS for a detailed discussion of the development of alternatives and the evaluation process, including project inputs, high-level assessment, and quantitative assessment.

8.9 CBIS Design Standards

For specific design standards applicable to all CBIS designs, planners should refer to the PGDS. Designs for new CBIS shall comply with the requirements set forth in the latest version of the PGDS, which continues to evolve. Project sponsors and design consultants are encouraged to review the PGDS applicability discussion in the General Information section to learn the version of the PGDS to which designs will be required to comply.

8.10 CBRA Design Standards

A CBRA provides the space and equipment required by TSOs to conduct:

- Level 3 searches of checked bags that have not been cleared by TSOs through Level 2 OSR
- Primary screening using ETD for unknown, OOG, and oversized bags from the BHS

The proper layout and furnishing of the CBRA are essential to ensuring that TSOs can properly, efficiently, and safely conduct the process of screening baggage. Careful consideration needs to be given to the operational controls, the ergonomic configuration, and to the equipment specified for the CBRA.

The PGDS includes baggage handling system functional requirements as well as physical requirements for CBRA designs. The CBRA should be viewed as office-type space for level of build-out finishes that provides a safe working environment for TSOs. It should be provided with the necessary infrastructure to ensure a secure and climate-controlled environment with adequate acoustic controls. For additional details on specific standards for the CBRA, planners should refer to the PGDS.

8.11 Trends

In the area of explosives detection equipment and baggage handling systems, there are very few short-term trends in terms of the operational and physical profiles of the equipment or the procedures. Most such changes in technology in recent years have come incrementally as technology evolves over significant periods of time. Typically, there are trade-offs between the throughput speed of the equipment, the ability of screening personnel to rapidly process the challenges facing them as the lines move through, and the capabilities of the passengers themselves to quickly divest and recompose in order to keep the process moving. At the same time, there are significant constraints imposed to maintain the optimum level of security through an appropriate mix of labor and technology.

EDS equipment must be large enough to accommodate luggage of all sizes, shapes, and configurations, while also providing the maximum probability of detection (P_d). All complementary technologies together must fit in a limited and sometimes inconvenient physical space. From an airport planning and design perspective, the physical size of the equipment is unlikely to change significantly, although the continual industry effort to improve the P_d capabilities and the rate of throughput may have the downstream effect of integrating several functions into a single technology, requiring less square footage, fewer lanes, and less queueing space to process an increasing number of people.

The airport planner must pay close attention to the mid- to long-term passenger growth projections, as well as the possibility of criminal or terrorist threats causing a significant change in regulatory requirements, which could potentially lead to a need to provide additional space and adaptability of supporting infrastructure and staffing.

Further, at the time of this writing, TSA has streamlined some of the acquisition and test and evaluation requirement processes, and is increasing interaction with the Original Equipment Manufacturer (OEM) through earlier involvement in the acquisition process. This increased interaction will encourage more mature technology through more transparent engagement with the OEMs on system architecture and testing. TSA is also evaluating high-speed EDS from several vendors with the expectation of adding them to a Qualified Products List by late FY2017-18.

8.12 Checklist

Baggage Screening Checklist

☐ Refer to TSA Design Guidance Document
- PGDS standards
- CBRA standards

☐ 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

☐ 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

SECTION 9: PASSENGER SCREENING CHECKPOINT

9.1 Passenger Security Screening Checkpoints

The intent of this section is to provide a description of the Passenger Security Screening Checkpoint (SSCP) equipment that exists, and the knowledge necessary to locate that equipment appropriately within the checkpoint in order to provide the highest level of security screening and efficiency, beginning at the queue and continuing through the composure area. The information included in this document should be used as a guideline when designing new checkpoints or reconfiguring existing checkpoints. All designs and reconfigurations must be coordinated with TSA Headquarters (TSA HQ), the local FSD and staff, and local airport stakeholders for adaptation to site-specific requirements. For specifics, review the most recent version of the full *TSA Checkpoint Design Guide* (CDG).

There are multiple layers of security in place at airports that facilitate the safe movement of people and commerce throughout the air transportation system. These layers are roadblocks to potential terrorist paths because they are equipped to detect and minimize threats that could occur within the system. Every airport and airport terminal building is unique in physical design and operational requirements. No single SSCP solution will work for every checkpoint, nor will it work for every checkpoint at the same airport. Every SSCP location must be reviewed as an entity within the overall airport security system. Improper SSCP design results in terminal and checkpoint queue congestion, long passenger wait times, flight delays, missed flights, and unnecessary security risks.

9.1.1 General Overview of SSCP

SSCPs are a critical element to an airport's overall terminal design, and should be considered during the development of the ConOps in the early stages of planning and conceptual layout. Performance requirements of an SSCP and airport/airline responsibilities are not included in this document. However, this information can be obtained from a number of TSA regulatory documents.

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 unsecured areas to the Sterile Area.

When designing a new terminal or checkpoint, or reconfiguring an existing terminal or 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 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 CCTV equipment (all addressed elsewhere in this document)

9.1.2 Regulations and Guidelines

The regulations governing airport security and passenger SSCPs include:

- 49 CFR § 1540 (Security: General Rules)
- 49 CFR § 1542 (Airport Security)
- 49 CFR § 1544 (Aircraft Operator Security)
- 49 CFR § 1546 (Foreign Air Carrier Security)

While the regulations do not define the specific technical requirements that govern design of SSCPs, they define in general terms what must be accomplished by the design. All TSA regulations can be obtained on the TSA website.

9.1.3 Essential Coordination

Key individuals from TSA HQ, local TSA (FSD) offices, government agencies, airport, and airline operations should be involved early during the SSCP design process. These groups will be able to facilitate dialog regarding local building codes, mutual aid agreements with local law enforcement/emergency responders, and joint commercial/military presence that could factor into the checkpoint design, especially during emergencies.

9.1.4 Planning Considerations

TSA equipment placement is intended to increase the level of security and improve the flow of passengers through the checkpoint. This is accomplished by providing adequate space for queuing of passengers, and to allow divesting and recomposure, which minimizes the occurrence of bottlenecks at the checkpoint. TSA HQ and airport designers collaborate to meet the latest CDG standards.

SSCPs are created by combining standard one- and two-lane module sets. These module sets are created based on standard TSA spacing for passenger ingress/egress, clearance for maintenance activities, and prevention of passenger breaches. Module sets should provide a controlled and contained screening environment where Sterile and non-Sterile Areas are separated from each other.

A modular design enables TSA to determine the depth and width needed for a particular number of lanes in each unique available space. The number of lanes required is based on a computational formula, taking into account several factors including the following:

- Capacity: Number of gates; number of passenger enplanements per aircraft (based on aircraft size and 100 percent load factor)
- Passenger Arrival Distribution: Based on the capacity analysis above, determine highest hourly peak rate of enplanements (flight schedules)
- SSCP Rates & Standards: Based on the arrival distribution analysis
- Transportation Security Equipment Capability

Most airports with international flights have a Federal Inspection Service (FIS) SSCP, where arriving international passengers are required to be screened before transferring to a domestic flight. The U.S. screening process has different requirements and provisions from the screening processes in many non-U.S. airports where a passenger may have originated. These are known as Last Points of Departure (LPD). The screening requirements for an FIS checkpoint are the same as other U.S. checkpoints, but the volume varies based on the frequency and capacity of inbound international flights.

9.1.5 Elements of SSCP

The intent of this section is to introduce all of the elements of a standard TSA SSCP. These elements can consist of hard materials, such as powered security screening equipment, and soft materials, such as non-powered ancillary equipment. For the most updated specifications on hard and soft materials, please review the most recent version of the CDG. The equipment in this section is described in the order that a passenger encounter it, from the non-Sterile Area to the Sterile Area. All elements of the system, no matter how seemingly insignificant, require an allocation of dedicated space as an individual moves toward the Sterile Area. The following descriptions are intended to capture all of the elements a passenger may encounter, but not necessarily at the same time, in the general order of occurrence.

9.1.5.1 Pre-screening Preparation Zone

The Pre-screening Preparation Zone begins as early as the curbside ticket counters and typically ends at the Travel Document Checker (TDC) podium, deep in the queue. This zone should incorporate architectural features of the airport and be designed to provide a calm environment for the passenger. Signage, instructional videos, and “ambassador” staff or volunteers, when available, should be used to reduce passenger stress and ease movement to and through the SSCP. Simple and effective signage that has been approved by the airport and integrated with their current signage policy can be used to direct and instruct passengers on screening requirements and procedures. Checkpoint signage can be coordinated with the airport’s specific architectural theme.

9.1.5.2 Queuing Space

The queue is where passengers stand in line at the front of the checkpoint on the public side. It is recommended that the queue be bounded by hard barriers along the perimeter with single strap stanchions defining the various lanes from the queue entrance(s) to the TDC(s). Queue lanes are approximately 400 to 600 square feet per lane, depending on the lane function and queue space available.

The queue should be big enough to meet the peak passenger load without interfering with other functions such as ticket counter traffic or checked bag processing in the lobby. The queue entrance(s) should remain open at all times when the SSCP is operational. Queues should be able to be cordoned off and funneled down to one TDC station during off-peak times.

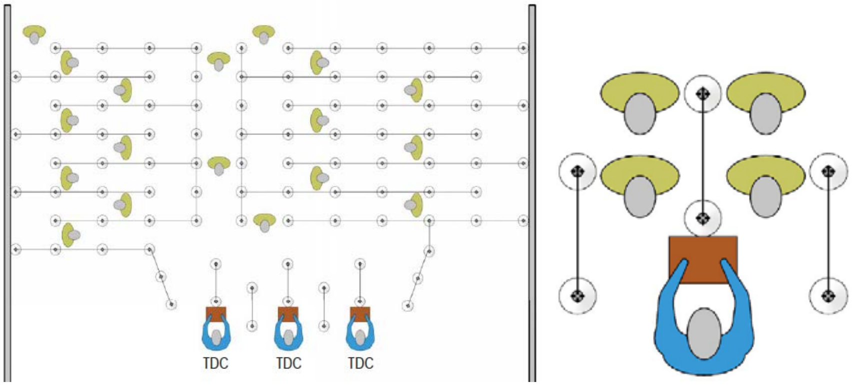
SSCP layout can affect the queue dramatically. When evaluating queuing space, airports should consult with local TSA on the current wait-time standard, as well as review the results of the analysis conducted for Capacity, Arrival Distribution, and Section 1d of the SSCP Rates & Standards. TSA also suggests estimating a minimum of 9 square feet per passenger. Planners should consider the possibility of extra space needed for such items as the K-9 program.

9.1.5.3 Travel Document Checker

TSA has the responsibility for reviewing credentials and verifying documents within the queue at the SSCP. This function is critical to the flow of passengers through the checkpoint, as it can be the bottleneck for getting passengers screened. The queue must be set up to properly feed the TDC podiums, and the TDC podiums must be set up to properly to feed the checkpoint lanes. The following guidelines should be considered when determining placement of the TDC and podium:

- The TDC should be set up so that no individual can circumvent or bypass the TDC podium.
- The TDC podium should be approximately 6–10 feet from the divest end of each lane in order to allow passengers to move freely toward their chosen lane.
- Alternating “mini-queues” on both sides of the TDC podium can be created by providing stanchions in front of the podium. This will force the passengers to form two separate lines for the same TDC. The TDC will process whichever “mini-queue” passenger is ready (refer to Figure 9-2).
- Airports can provide appropriate power and data infrastructure for such equipment as Credential Authentication Technology (CAT), and Boarding Pass Scanners (BPS), as reflected in the CDG.

Figure 9-1. TDC with Alternating "Mini-Queues"



Source: TSA

9.1.5.4 Carry-On Baggage

- Carry-on bag screening is mandatory at an SSCP. This screening process is accomplished by Advanced Technology (AT) x-ray machines that have the following components: Loading table / entrance roller conveyor
- In-feed tunnel
- Scanning belt (continuous from in-feed to out-feed tunnel)
- X-ray dome
- Out-feed tunnel including alarm bag cut-out
- High speed conveyor and tunnel
- Extension rollers and/or exit roller

Interpreting the bag images on the monitor requires focused concentration by the Transportation Security Officer (TSO). The operator should have an ergonomic and distraction-free environment. The space should be designed to minimize glare on the monitor from interior lighting, glass walls, or sunlight, keeping in mind that the AM/PM glare will differ depending on orientation. The monitor height should be at an optimal viewing angle. The operator must also have a clear view of the machine’s entrance and exit conveyor. Columns, power poles, and signage, etc., should not prevent the TSO from seeing the bags going in and out of the x-ray unit.

Equipment determination for each lane at an SSCP will be based on the space available, the required number of lanes based on passenger load, and the floor structure. If the checkpoint is being reconfigured, additional consideration should be given to the location of the existing electrical outlets, TSO familiarity with a specific manufacturer or vendor, and existing maintenance contracts. The TSA HQ point of contact, local FSD staff, and the checkpoint designer will need to work together to determine the best solution based on the site conditions.

9.1.5.5 Walk-Through Metal Detector

The Walk-Through Metal Detector (WTMD) is an electronic archway used to detect metallic weapons and/or metal contraband concealed on a person. Currently, only the original equipment manufacturer (OEM) and designated maintenance contractors are certified and authorized by TSA to relocate, recalibrate, and service the WTMD.

9.1.5.6 Barriers and ADA Gates

In order to prevent passengers and/or items from passing into the Sterile Area from the non-Sterile Area without being screened, barriers and/or Americans with Disabilities Act (ADA) gates should be installed to close all gaps exceeding 12 inches across the front width or façade of the checkpoint.

The ADA gate is part of the line that separates the non-Sterile Area from the Sterile Area. However, the ADA gate can allow passengers who cannot otherwise pass through the WTMD to reach the Sterile Area.

9.1.5.7 Advanced Imaging Technology

The implementation and operation of Advanced Imaging Technology (AIT) systems as the primary screening method maximizes the likelihood that TSOs will detect potential threats while preserving passengers' privacy. The use of AIT has brought a shift away from solely metallic-based threat detection and toward organic threats placed on the body. Incorporation of this and other evolving technologies into the checkpoint environment is part of a layered approach to the dynamic SSCP SOP for primary passenger screening.

One such approach is TSA PreCheck, which creates a dedicated lane for pre-cleared passengers who have voluntarily gone through a security background check. Being deemed as significantly lower-risk persons, the screening process in the PreCheck lane, although still technology-based, is less rigorous and much faster. Reconfiguration of one or more such lanes typically means the loss of a regular lane, which may or may not affect peak load throughput times and staffing requirements, and require significant infrastructure adjustments.

9.1.5.8 Explosives Trace Detection, Bottle Liquid Scanner, Alternate Viewing Station

Secondary screening areas are required for clearing passenger carry-on items when the primary screening at the x-ray raises concerns. Secondary screening areas typically consist of an Explosives Trace Detection (ETD) device and a Bottle Liquid Scanner built into a mobile cabinet, stainless steel bag search tables, and an AVS away from public view.

9.1.5.9 Private Search Area

A private screening room should be located at the back end of the checkpoint in the Sterile Area. The area should be available to accommodate passengers who request private screening instead of being out in the open. The private screening room should be opaque. However, an alternative modular system or stud-wall room near the checkpoint could be used for private screening. The location of the private screening area within the checkpoint should be as centralized as possible, to minimize the walking distance for passengers and TSOs, without causing congestion or impeding traffic flow in and around the checkpoint.

9.1.5.10 Egress Seating Area

Egress seating at the Sterile side of the checkpoint is used for passengers to sit down and recompose themselves with their personal belongings after completing the screening process. This area is usually out of the main passenger flow.

9.1.5.11 Supervisory Transportation Security Officer Podium

The Supervisory Transportation Security Officer (STSO) should be able to perform administrative duties while periodically viewing the entire screening operation with minimal obstructions. The STSO should be located in an optimal location away from the passenger flow, such as the in back or on the side of the checkpoint. Please see the CDG for further guidance.

9.1.5.12 SSCP Adjacent Walls and Boundaries

Set boundaries for an SSCP will be established per CDG requirements and the ASP. The SSCP length starts at the TDC podium(s), extends through the checkpoint elements discussed in this section, and ends at the checkpoint exit, which could be adjacent to the egress seating area, STSO or LEO podium. The SSCP width is the wall-to-wall width of the checkpoint, including all the screening lanes and any co-located exit lane. All walls adjacent to the non-Sterile side need to be at least 8 feet high to prevent the passage of prohibited items from the non-Sterile Area to the Sterile Area. Designers should incorporate a means to secure the SSCP when lanes not in use or the SSCP is closed. In the future, new technology may extend the boundaries of the SSCP to include additional equipment and functions within the checkpoint, or equipment and functions located remotely within the airport.

9.1.5.13 Exit Lane

An exit lane is often co-located with a checkpoint, or it can be located independently. This lane should be easily identifiable without adversely affecting security, and adequately sized for deplaning passengers exiting the concourse. All building code egress path requirements must be met. This issue is discussed in more detail in Section 10 Access Control Systems of this document.

Prevention of a security breach through an exit lane, whether co-located near an SSCP, or non-co-located (remote from the SSCP), has historically required the use of a guard, whether employed by TSA or sub-contracted through a security guard service. Since TSA has declared exit lanes to be an issue of controlling access into the Sterile Area, responsibility has shifted primarily to the airport operator.

The typical functions should allow passengers an unimpeded means of egress from the Sterile concourse to the non-Sterile landside. A functional system may consist of:

- Airside doors that automatically open when passengers approach the exit
- Landside doors that automatically open to allow passengers to enter the non-Sterile Area
- Landside intruder detection technology that detects and records the intrusion, provides alarms to the intruder and signals to security personnel that initiates lockdown features
- Safety features that prevent moving door panels from causing pedestrian injury
- Digital monitoring to detect objects left in or thrown from landside to the airside
- Input and output connection points for integration to local Physical Access Control System (PACS)
- The ability to change from a high capacity throughput mode to a low capacity interlock mode for higher levels of security with reduced throughput

9.1.6 SSCP Power and Data

The power and IT requirements for security screening and ancillary equipment is unique in regard to each circuit type, receptacle type, and quantity of data drops required. Location of the electrical and data outlets in reference to the equipment is also critical. Familiarity with these requirements will be essential when designing a new checkpoint or reconfiguring an existing checkpoint. For detailed specifications and requirements, please refer to the most recent version of the CDG, *Electrical and Data Future Planning Guide,* as well as Section 13, Communications, IT, Power, and Cabling on IT and power requirements.

9.1.6.1 Equipment Requirements, Receptacles, and Locations

Circuits from existing electrical panels should be used, when available, as indicated by the panel board and corresponding panel schedule that serves the checkpoint. Often, the panel schedule lacks sufficient detail with regard to what equipment is powered by each circuit.

Most of the new technology requires a dedicated circuit and multiple data drops; therefore, non-dedicated loads should be grouped together when possible in order to free up dedicated circuits. All dedicated circuits are not to share the ground wire. The checkpoint designer should not assume an existing circuit is dedicated, or expect the electrical contractor to trace an existing circuit and remove any excess load. For future checkpoint build-outs, dedicated circuits and data drops should be provided for all security screening equipment. There will also be data and electrical requirements for TSA leased and non-leased space at the checkpoint, and for an IT cabinet and fiber optic runs to the cabinet.

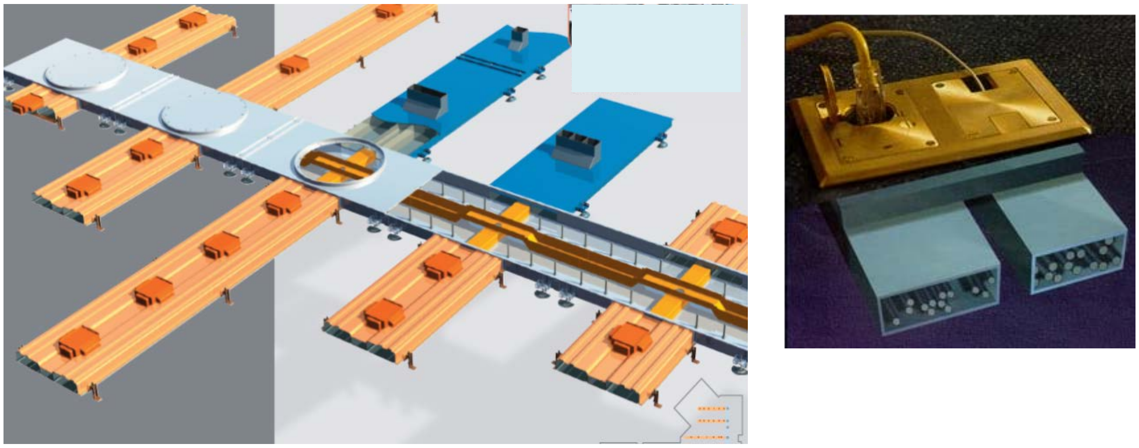
New electrical panels may be required for new circuits in support of a new checkpoint or reconfiguration of an existing checkpoint. This requirement will be determined during the design phase by an electrical engineer. The electrical design of a new checkpoint or reconfiguration of an existing checkpoint must meet national and local codes in addition to any airport, state, county, and/or city requirements, depending on the authority having jurisdiction. Uninterruptible power supply (UPS) backup power is not required for SSCPs, although it may exist or be required at some sites. Power and data receptacles should be of high quality industrial standard to accommodate high volume traffic through a SSCP. All power/data poke-through devices (flush or recessed), pedestals/monuments (surface-mounted boxes, i.e., “tombstone”), power poles, fittings, and/or plates must be coordinated with the airport operator and the TSA. In addition to receptacle type and finish, the airport should approve core drill sizes and locations of electrical trenches. Poke-through and pedestal receptacles should be positioned in such a way as to avoid trip hazards for both passengers and TSA personnel. Extension cords for permanently installed equipment are unacceptable if the equipment cord is too short to reach a receptacle. One preferred method of running electrical and data in new construction is in a Walker duct/trench system as illustrated in Figure 9-3 below. This may not be feasible in existing construction.

- Benefits
  - a) Large capacity for routing wiring and cables beneath floors
  - b) Cost savings for drilling and x-ray of floors every time a core drill is needed or relocated
  - c) Provides easy access to wiring and cabling in the floor with removable panels for access though the raceway
  - d) Flexible construction using modular components to create a floor duct system or raceway
  - e) Future needs met without disturbing floor by relocating/adding/removing components
  - f) Use separate compartments per electrical code and specific needs—i.e., separation of power and data wiring
  - g) Typically comes in four (4) widths—6", 12", 18", and 24"
  - h) Typically comes in two (2) depths—2-1/2" and 3-1/4"
  - i) Load capacities as follows:
    - o 6" width no supports—up to 2400 lbs concentrated load
    - o 12" width no supports—up to 2400 lbs concentrated load

  - 18" width one support row—up to 2000 lbs concentrated load
  - 24" width one support row—up to 2000 lbs concentrated load

- Installation Considerations
  a) Requires cutting a floor trench to install in an existing concrete floor slab for use in new construction
  b) Requires coordination of the installation with structural components in a floor slab, such as reinforcing rods, steel, existing in-floor devices, and conduits ; in some cases, power in the floor, as well as underground rail transport, have been known to cause interference

Figure 9-2. Example of Power and Data Under-Floor Distribution



Source: TSA

9.1.6.2 SSCP Lighting

Lighting requirements for a new checkpoint should meet national codes, and ideally meet the minimum luminance level of 30 foot candles (fc) as defined by ANSI/IESNA RP-104. In some cases, this requirement may be higher when the minimum is set by local building codes.

Additional lighting may be required for any SSCP that has CCTV cameras to monitor activity. See Section 12 of this document regarding CCTV and lighting.

9.1.6.3 CCTV

Cameras at the SSCP increase the public's sense of security in deterring theft by capturing visual records of suspicious activity. Cameras are particularly helpful for continued surveillance at unstaffed or closed checkpoints. The number of cameras will vary depending on the size of the checkpoint, obstructions within the checkpoint, lighting, and the quality of the CCTV system. A sufficient number of cameras should be employed to cover each lane, all secondary screening areas, and co-located exit lanes. Cameras should not intrude on passenger privacy by locating them in the AIT Remote Viewing or Private Screening Room. Cameras should be positioned to show the front view of a person's face and any other identifying characteristics. For more information, see the *TSA Baseline Video Surveillance Functional Requirements* for Checkpoint.

9.1.7 Safety

SSCPs must not only screen passengers and their carry-on baggage, but do so without compromising the safety of either the passengers or the TSOs conducting the screening. Safety requirements and safety-related considerations should be built into the SSCP design from the beginning, and should be treated as an integral part of the design process. The standard checkpoint layouts in this document are intended to provide good starting points, but safety Subject Matter Experts (SME) should be included in every phase of the design to provide input on conceptual plans and/or construction drawing packages.

9.1.8 Designing for the Future

Airport security technology is a dynamic and rapidly changing field. Although an airport may be designed to take maximum advantage of the current technology, those designs should be sufficiently flexible and adaptable to meet changing threats and support the equipment that will detect them. Security screening equipment dimensions and/or processes may change, requiring the entire airport security management team to make important decisions regarding modifications, which the designer must then accommodate. The designer's task will be easier if the original design has anticipated the need for change and allowed for size and space adjustments by surrounding the SSCP with as much flexibility and potential expansion space as possible. Please see the *Innovation Supplement* for further information.

9.2 Trends

Trends in planning and design of the SSCP closely parallel those of the baggage handling systems —in both cases, they require close cooperation with the TSA to meet their technology and staffing requirements, close attention to current and anticipated passenger load predictions, a firm understanding of the airport's master plans in such areas as new or extended terminals, and readiness for changes in air carrier locations and service (i.e., international versus domestic gates and/or concourses), which can significantly affect the locations, sizes, and operational requirements of checkpoints.

TSA PreCheck lanes are now fully operational at many airports, but it remains to be seen whether future enrollment and usage patterns will sustain TSA projections. Further, while still in the experimental stages at this writing, recent changes in TSA requirements for co-located exit lanes have dramatically changed airport responsibilities towards exit lanes that are adjacent to the checkpoint, and are changing some airports' approaches to implementing non-co-located exit lanes.

Other technology innovations are currently in the investigatory stages, such as RFID tags on both checked and carry-on baggage to speed their passage through the checkpoint and the baggage distribution process. At the time of this writing, TSA has already placed a pilot installation of automated screening lanes in the field at a major airport. In these, motorized rollers carry significantly larger bins with RFID tags past overhead camera arrays so that all the passenger's possessions can be consolidated and more easily associated with that passenger for automated diversion to accommodate any necessary secondary screening. This concept is designed to significantly increase checkpoint throughput.

9.3 Checklist

SSCP Design Checklist

- □ Refer to primary TSA guidance documents, including CAD blocks (consult TSA for the most up to date versions)
- □ Consult with TSA HQ Checkpoint Designer, airport, and airline

□ 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 travel lane
  - Checkpoint boundaries

□ SSCP signage

□ Space for TSA staff

□ SSCP layout and spacing standards

□ Designing for the future

SECTION 10: ACCESS CONTROL SYSTEMS

10.1 Introduction

This section is a summary of the RTCA DO-230-G document, *Standards for Airport Access Control Systems*, which is updated periodically as technologies, regulations, and operational requirements change.

This document provides detailed structured guidance on industry best practices and conveys TSA requirements for airports; it was developed as an industry reference on developing cost-effective access control systems that meet the needs of all stakeholders. Extensive in-depth information on implementation of an airport access control system is included and is updated regularly. The document is available from the RTCA.

The purpose of an access control system at airports is to deny access to unauthorized persons and to control the passage of staff into Secured and Sterile Areas in line with the regulatory requirements of 49 CFR § 1542 and the airport's specific Airport Security Program (ASP). These systems are only required for TSA-regulated airports.

Airport access control systems are not designed to control the access of passengers to Sterile Areas, and specifically not for "Trusted" or "Registered" traveler programs, or cabin crew staff via programs such as "Known Crew Member."

Access control systems are normally considered in two parts: the first provides the vetting, approval, and credential issuance process; the second is a physical access control system that uses the resulting credential to provide or deny access.

Access control systems were originally designed to automate physical access controls, and have subsequently accommodated a personnel credential issuance process. U.S. commercial airports must meet requirements to control access, but vary widely in approach and technology based on their infrastructure, resources, operational requirements, public administrations, and variances in local/state laws and regulations.

Certificated airports with capable access control systems issue credentials to be registered into the Physical Access Control System (PACS), to allow unescorted access to security-related airport areas for staff, tenants, and other authorized users (law enforcement, first responders, construction personnel, etc.) when necessary.

Any subsequent changes in credential status (active, invalidated, etc.) and/or access privileges must be communicated between the credentialing and PACS programs in a timely and secure manner.

10.1.1 Regulatory Requirements Overview

The regulatory requirements are specified in 49 CFR § 1542. However, airport staff access control systems 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.

Each airport's access control systems and procedures are detailed, from an operational perspective, in each airport's federally mandated ASP. These programs are also designated SSI to only be shared on a "need to know" basis.

Note that airports exclusively serving GA are not currently required by regulation to have such access control systems, although deployment of one is considered an industry best practice. TSA operational security guidance for GA can be found https://www.tsa.gov/for-industry/general-aviation.

GA facilities at regulated airports must comply with the airport's overall security requirements in the airport's ASP. See Appendix D of this document.

10.1.2 Performance Criteria

Airport security systems should be high availability systems operating 24/7/365. System availability should meet or exceed 99.99 percent; higher performance requirements should be considered for higher risk airports.

10.1.3 Selectivity

Under current regulations, distinct security zone criteria are defined for airports; their specific locations and boundaries are detailed in each airport's ASP.

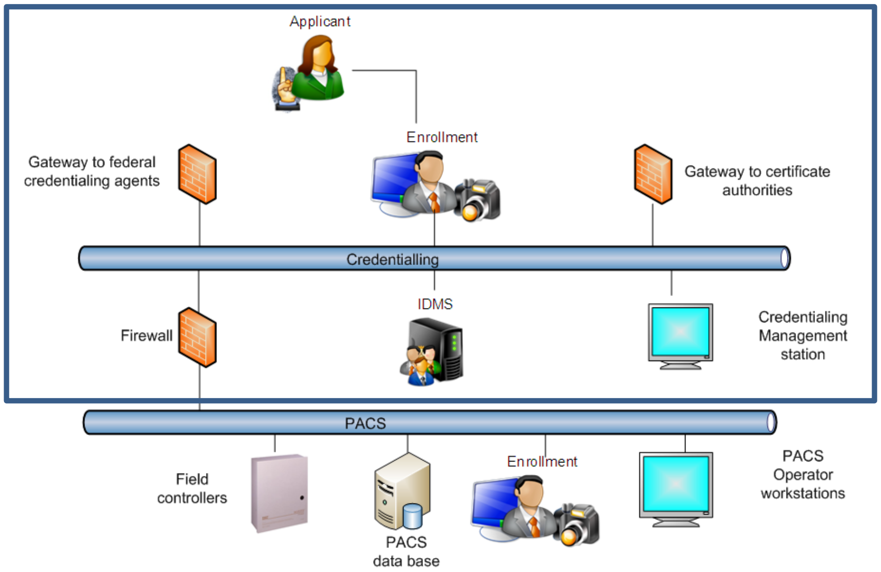
These security zones are the Sterile Area, Secured Area, SIDA, and AOA, which correspond respectively to security measures for interior terminal areas past screening checkpoints (Sterile); exterior airside areas where aircraft are docked or parked (Secured); airside areas requiring security ID display (SIDA); and the airfield itself, which includes runways and taxiways (AOA); as well as terminal and cargo ramp areas, which may include more than one such area.

These definitions are subject to regulatory change. A system should be flexible enough to support changes to the control and monitoring of access to any airport areas, and should also be capable of supporting additional areas which may be so designated by regulation, Security Directive, or by an operational decision of the airport.

10.2 Credentialing

Credentialing is the process by which an individual is issued a credential that visually (and in some cases electronically) identifies the person as having been granted privileges for unescorted access to Secured and Sterile Areas on an airport. Components used for credentialing are shown in Figure 10-1.

Figure 10-1. Credentialing System Components (Simplified)


Applicant
Enrollment
Gateway to federal credentialing agents
Gateway to certificate authorities
Credentialling
IDMS
Firewall
Credentialing Management station
PACS
Field controllers
PACS data base
Enrollment
PACS Operator workstations

Source: RTCA 230

10.2.1 Credentials

Airport credentials are normally in the form of a conventional ID badge, often called a SIDA badge. The credentialing process, which is determined by both federal and local regulations, typically has the following requirements:

- Determining an applicant’s identity through scrutiny of an applicant’s official identity documents
- Verifying the applicant’s identity and biometric information by a regulatory clearance process to determine if that individual is qualified to have access privileges
- Collecting the individual’s fingerprints and biographical data for conducting a Criminal History Records Check (CHRC) and a Security Threat Assessment (STA) that checks against a number of federal databases
- Conducting a similar check against state or local databases (only required for some locations)
- Conducting airport specific security training of the applicant
- Issuing a credential along with appropriate access privileges for that facility

It should be noted that, while an applicant’s fingerprints must be submitted to federal authorities for checks against criminal records in order to obtain the required clearances, an operational access control biometric of any type (apart from a facial image on a badge) is not currently required by federal regulations for airport access control systems, although some airports have chosen to implement them to provide an additional access control factor and hence enhanced security.

The above process can identify people who, on the surface, are not entitled to an airport badge; thus, there is need for an adjudication process in the event of a negative determination at any stage. The badging or credentialing process as a whole is subject to significant recordkeeping and audit requirements, which may be inspected by the TSA.

There is no national credentialing system; therefore, individuals must be approved at each airport separately, even if they have credentials from other airports.

In addition, each airport has an airport-specific mandatory airport security training program that each individual must complete before being issued an airport credential. The type of training typically depends on the nature and scope of access permitted, including special training for persons with ramp-driving privileges.

10.2.2 Inter-airport Credentialing Interoperability

The concept of an interoperable credential has been raised, which would make it unnecessary for individuals with the requirement to work at more than one airport to be separately processed for each airport, such as airline staff (and also for first responders and mutual aid personnel). At one time, this was a long-term TSA goal. However, due to the legal and operational challenges, plus the effectiveness of the current systems, this policy is no longer actively pursued.

10.3 Physical Access Control Systems

PACS allow or deny entry to Secured and/or Sterile Areas of the airport on the basis of a credential issued by the credentialing process.

PACS usually involve a computerized system of credential readers, (normally but not always badge readers), automatic door locks, and perimeter portals located throughout an airport. Only individuals with airport-issued or airport-approved credentials with appropriate permissions can pass through these access portals and enter Secured and Sterile Areas.

However, at smaller airports, PACS could also be based on simple lock-and-key methods and/or physical guards.

Normally, all but the smallest airports use an electronic access control system of some sort. PACS have three main operational requirements:

- Monitor access to the Secured and Sterile Areas
- Annunciate access violations/access to areas made without an appropriate credential
- Record and log all pertinent events, and provide reports as necessary

10.3.1 Access Credentials

To meet the regulations there are two types of credentials:

- An identity credential (typically an ID badge) used to verify the individual’s identity (and potentially to verify security clearances in the future)
- An access credential (typically a badge or a fob), or in combination with the ID badge, by which the access control system will allow entry to secure areas at a specific airport

These credentials need not be the same, but are usually incorporated into a single badge for accountability and user convenience.

10.3.2 Monitor Access

The primary purpose is to automate the process of allowing authorized individuals access to specific Secured and Sterile Areas, and denying access to unauthorized individuals, generally 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 system verifies whether the owner of the credential is entitled to enter, and either unlocks it to allow passage, or denies passage and provides a local alert of this denial to the airport security staff, which is typically housed at a Security Operations Center (SOC).

The same credential can also be used at staffed security portals (i.e., vehicle gates, etc.), and can incorporate a PIN and/or biometric as an additional authentication factor.

Many airports also use such credentials to control access to the AOA and other areas not designated as Secured Areas, as well as to airport administrative and non-public areas.

10.3.3 Annunciate Access

Access violation notifications are sent to the SOC whenever persons enter Secured or Sterile Areas without permission, and (normally) when repeated attempts are made to enter an access point regardless of denial of access.

This annunciation can be accomplished by means of a local alarm at the door, and/or remotely at a command center or SOC where staff can monitor alarms and dispatch appropriate response personnel to the scene.

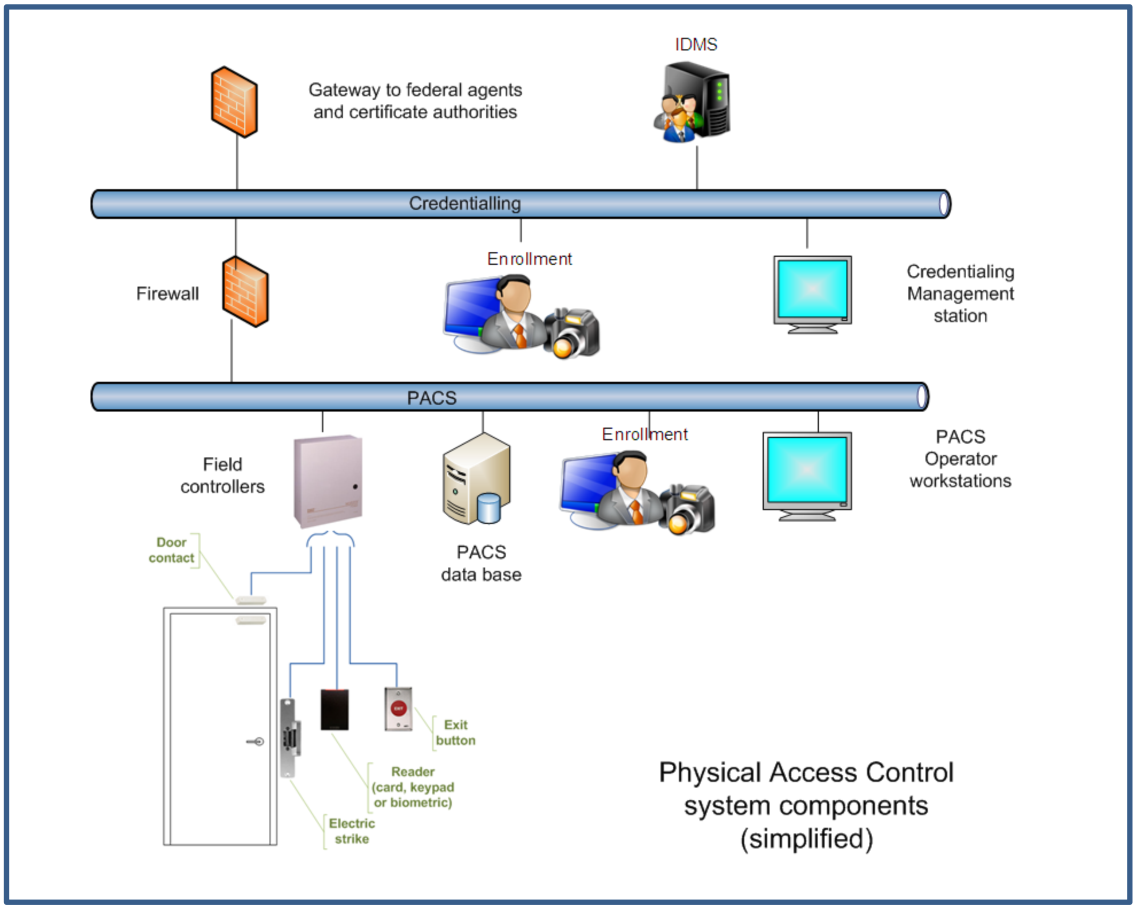
10.3.4 Record and Report

Access attempts into Secured and Sterile Areas, whether successful or not, should be recorded to provide reports as required. Such data should be kept for a period of at least 12 months, or as defined in the ASP.

10.3.5 Typical PACS

The components of a typical PACS are shown in Figure 10-2.

Figure 10-2. Physical Access Control System Components (Simplified)


IDMS
Gateway to federal agents and certificate authorities
Credentialling
Enrollment
Firewall
Credentialing Management station
PACS
Field controllers
Enrollment
PACS Operator workstations
PACS data base
Door contact
Exit button
Reader (card, keypad or biometric)
Electric strike
Physical Access Control system components (simplified)

Source: RTCA 230

10.3.5.1 General

A PACS typically consists of three main components:

- Portal hardware: Portal hardware includes card/badge readers and portal locking/unlocking hardware mechanisms and switches. These are conventional components that are common with almost any PACS.
- Field controllers: Field controllers (or field panels) are typically microprocessors that control and manage several portals. Typically, these devices contain a partial database of local cardholder and privilege information, and provide a degree of standalone operation should any communication links to the central server(s) be lost. These units are normally supplier specific and cannot easily be mixed with another supplier.
- Central servers: The central server(s) contain the access control system primary database and is used to perform administrative and transaction recording (logging) functions and other centralized functions, using supplier-specific application software.

The databases and functionality can be duplicated or distributed if required for redundancy purposes. The central server can also perform monitoring functions, and can be connected to separate systems or integrated with other systems such as CCTV.

Operator monitoring functions are typically performed on computer workstations with large display screens, but can also be integrated within a full-scale security control center. These operator(s) can monitor the system status, and receive and process events and alarms.

10.3.5.2 Biometric Readers

Some airports have opted to use biometrics as an additional method of user authentication (or access control factors) in their PACS.

This means that in addition to a conventional badge or credential reader there is a biometric sensor device with software algorithms that collect and compare the credential holder's biometric characteristics with the biometrics previously enrolled in the system.

The majority of airports using biometrics have chosen to implement fingerprint technology since fingerprint is the most mature and field-tested biometric with the widest choice of vendors, competitive prices, and published standards.

It is not necessary that all access portal readers have such a biometric capability. Biometrics could be incorporated in readers only in those entry portals determined to be high risk, or might be activated only during elevated risk conditions.

As a result, some airports may deploy only a small number of biometric-enabled readers, while others may deploy such readers more widely. Relying on swipe or proximity cards, even with the addition of a badge and PIN function (which is an alternative additional access control factor in use at many airports), is less secure because there is no assurance of the user's identity.

10.3.5.3 Mobile Credential Readers

An increasing number of airports are deploying mobile credential readers. These allow on-the-spot verification of an individual's airport credential, independent of the network of fixed badge and credential readers around the airport. These readers can electronically verify the credential, and can also hold a biometric of the person to whom each credential was issued to add a further level of verification.

10.3.5.4 Use of Personal Identity Verification Credentials

If an airport decides to utilize a Personal Identity Verification (PIV) credential for federal workers and contractors (with or without a biometric), additional system and operational requirements may ensue.

Essentially, the reader will need to read and process the various data objects on the PIV card according to the technical specifications associated with the *Federal Information Processing Standard (FIPS) 201*, which could require an internet connection to each portal reader with access to a Public Key Infrastructure (PKI).

An alternative could be to perform periodic certificate validation for those registered card holders through the central server during idle time or in background mode.

Use of true PIV cards is also possible, but is currently not widely deployed. However, it should be noted that handheld portable devices that are now commercially available are designed to function with interoperable smart cards based on FIPS 201 for PIV of federal workers and contractors, which could be used for first responders.

10.3.6 Support Requirements

Access control systems at airports typically have three major support requirements:

- Power
- Communications
- HVAC

10.3.6.1 Power Requirements

Power should be provided via a UPS, which is sized for a specific load and operating duration. For additional loading and longer durations, backed-up power should be provided by engine-generator sets to ensure continuous operation even during an extended power failure.

Failures and significant events affecting power should be annunciated at the airport SOC even if there is a separate maintenance monitoring capability available.

In general, access control systems have power requirements for three devices:

- Central server(s): Servers are usually located in a main equipment room, which typically has both backed-up and UPS power available. Access control system servers and communication controllers do not typically require large amounts of power, but their requirements need to be factored into the total power requirements. A UPS for a processor should provide at least 4 hours of system service after main power failure.
- Field controller: Field controllers are usually located in communication closets, which should be placed in Secured Areas and only be accessible to authorized personnel or be under continuous surveillance. A UPS for a field controller should provide at least 4 hours of system service after main power failure.
- Portal or reader device: There are two types of door and portal devices: those that require little power, such as door sensors and credential readers, and those that require more power, such as magnetic locks. If power is required to such low-power devices, (typically but not always 24V dc), it is either generated locally from a backed-up supply or centrally at the nearest closet via a UPS.
- Magnetic locks have a more significant power draw, and provision of UPS capability can be a design issue; but at least 20 minutes should be provided. There may be fire code regulations for the use of magnetic locks on some doors.
- Currently, power over Ethernet can support sensors and ID media readers if these devices are on IP-based communication. Otherwise, conventional low-voltage wiring from the communication closet is required.
- Some access system devices will be located on the perimeter or at other remote locations; these sometimes bring special power challenges and opportunities, such as use of solar power. Each location should be assessed according to its own circumstances.

10.3.6.2 Communications Requirements

On-site airport PACS communications require three components:

- Linkage between devices at portals to field controller panels
- Linkage between field controller devices to a central server
- Linkage to any regulatory agencies or credential clearing services

On-airport Backbone Infrastructure
Airport PACS generally employ a standard IP-based backbone communication structure that enables shared communications with the central server, which typically hosts the access control database, field panels, and monitoring stations.

Secondary Infrastructure
Secondary infrastructure is the links from the local panels to devices.

In the past, proprietary standards and legacy communication systems from local control panels to devices and door controllers were deployed, which typically could not share a common communication infrastructure. Newer systems, which use IP-based secondary communication structure(s), are fully capable of sharing a common infrastructure.

Where common secondary infrastructure is not available, appropriate wiring is typically the responsibility of the access control system supplier.

Off-airport Communications
Initially, airport access control systems were typically closed systems (i.e., without connection to the internet or the outside world). However, the credentialing component requires such links.

These systems include fingerprint live-scan systems, and have a direct communication link to the federal agency and/or service provider.

More recently, requirements to interface related credentialing systems with DACs and/or federal agencies has led to directly connected systems to eliminate the requirement for redundant data entry.

These typically use standardized virtual private network (VPN) structures and not conventional internet connectivity services.

Though initially separate systems, PACS and credentialing systems now frequently share secure controlled links between the two components enabling the automated sharing of data and minimizing the need for re-entry of data. These links need to have appropriate cyber protection.

Given the abundance of cyber-attacks on government and other secure facilities, airport operators must remain vigilant when considering links to any external systems, including other airport IT systems, and federal, state and local agency systems.

Use of Onsite Shared Communications Infrastructure
A separate infrastructure should be deployed to maintain a high level of security appropriate for access control and alarm monitoring systems.

This requires physical separation of control for the fiber and copper components of security systems, due to the inherent risks associated with sharing such a network with conventional IT systems.

However, some airports have taken the step of sharing such a network with other security systems, such as CCTV, where the risk is substantially reduced, and they have separated the applications at the cost of some increased administrative complexity.

A common issue is that while conventional IT systems require frequent upgrades and reconfiguration, access control systems generally do not. This can lead to issues of incompatibility if non-security systems share the same physical network.

Use of Wireless Technologies
Wireless technology is convenient and often less expensive to deploy than conventional technology, but it has inherent risks.

Any omnidirectional transmission, (in which the majority of Wi-Fi type systems are included), is at risk from a "denial of service" attack, and also monitoring, even if the best possible security and encryption measures are deployed. Even the best wireless encryption is still not completely secure. Thus, wireless transmission should not be used for critical transmission wherever possible.

Point-to-point unidirectional wireless links do not suffer from these problems to the same extent. Free space optics, which use transmissions at a different frequency, are even more secure, but do not operate efficiently in all weather conditions.

Short range wireless technology, such as Near Field Communication and other technologies, is becoming increasingly available, and some suppliers provide levels of security appropriate for airport use.

Maintenance Considerations
Modern communication technology offers a wide choice of devices and options. However, these can come with maintenance and administrative complexity. Smaller airport operators may wish to consider whether this complexity is worth the added benefit.

Perimeter Devices
Some access system devices will be located on the perimeter or other relatively remote locations with special communication challenges. Each location should be assessed according to its own circumstances.

Monitoring
System failures and significant events with communications should be displayed at the airport SOC.

10.3.6.3 Environmental/HVAC Requirements

HVAC needs are often overlooked. Some communication switches and servers can generate significant amounts of heat, which can adversely impact an installation's environment.

The impact of any new equipment's heat generation or cold tolerance should be identified, as well as the existing HVAC capabilities of any room, closet, or outdoor environment.

In addition, although field panels typically have very good temperature endurance characteristics, in extreme areas these also may require heating or cooling. The same considerations apply to video cameras.

10.3.7 Special Device Considerations

Some security devices have special requirements.

- Anti-tailgating Devices: Anti-tailgating strategies may employ specialized systems and equipment to prevent multiple entries into a Secured Area based on a single credential. These may apply to perimeters, airfield, external facilities, and other security-related areas (security equipment rooms, data centers, bonded/sensitive/restricted areas, etc.)
- Anti-tailgating systems and equipment include devices such as turnstiles, readers, mantraps, air locks, and various sensors and surveillance capabilities (guards, CCTV, video analytics, etc.)
- ADA Issues: Airports are required to be compliant with the Americans with Disabilities Act of 1990 (ADA). This may require additional equipment and 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 Issues: In general, fire detection and alarm systems can be integrated with access control systems. Features often include the use of crash bars on fire exit doors linked to the access control system to detect unauthorized operation.
- During an emergency, these doors may be accessed from public or Sterile Areas directly to Secured Areas and the 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 access from public to Secured Areas. However, some unique circumstances may not always make this possible, and dual use elevators are not uncommon. In the event of dual use, access to the Secured and Sterile Areas need to be under the control of the access control system wherever practical.
- In addition, 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 secure floor without warning or positive controls.
- Environmental Requirements: Use of access control systems inside facilities presents minimal environmental challenges. However, having systems deployed outside or in exposed baggage handling areas with dirt, dust, heat, or snow presents some challenges to the electronics and the actual operation.
- 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 PACS. This can be particularly challenging.

10.3.8 Integration with Other Systems

Security systems with which access control system integration is typically required include CCTV, perimeter surveillance and sensors, duress alarms, and others identified below. Each is addressed in more detail in related sections of this document.

- CCTV: CCTV is widely used with access control systems in order to effectively monitor access portals. Details of video surveillance requirements are given in Section 12, Video Surveillance, Detection, and Distribution Systems.

- Perimeter Intrusion Detection Systems (PIDS): PIDS are designed to monitor and detect vehicles and persons transiting the airport perimeter. Numerous perimeter intrusion technologies are available and have been customized for particular facilities (i.e., fuel farms, cargo areas, etc.) See Section 11.
- Duress Alarms: Duress alarms can be installed at various locations throughout an airport. This includes checkpoints, but could also include dispatch offices, Customs and Border Protection (CBP), and the check-in and ticket counters. Location and installation of these devices is airport and operational model dependent. These devices are usually linked into an access control system to provide a common annunciation point for operations.
- Vehicle Gates: Vehicle gates are described in Section 4, Airport Layout and Boundaries. Due to the regulatory requirements and Security Directives associated with security gates, there is a clear requirement to link these back to the airport access control system to provide the same level of control and response as at standard portals.
- Baggage Handling Explosives Detection Systems (EDS), Explosives Ordinance Disposal (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 prevent theft and interference with equipment. This decision should be based on local conditions and operational practices.
- Screening Checkpoint Issues: Passenger screening checkpoints present some unique challenges for access control.
    - First is the need to secure the checkpoint and the access route via the checkpoint when it is not in use. This typically requires locking doors or rollup mesh screens. The checkpoint may be locked from one side or both depending on the airport configuration. Such doors should be controlled and monitored by the airport access control system. Reduced checkpoint lighting during periods of inactivity may impact the surveillance camera performance.
    - 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.
    - Third is the issue of the exit lane. Prevention of a security breach through an exit lane, whether located near or remotely from the checkpoint, has historically required the use of a guard, whether employed by TSA or contracted through a security guard service. Technologies now exist to handle such exits without a local guard.

10.3.9 Federal Inspection Services Device Requirements

Federal Inspection Services Areas, primarily CBP, are another category of security area. The requirements for security and the delineation of these areas is described in Appendix C and found in greater detail in the CBP *Airport Technical Design Standards*.

This CBP publication lists specific requirements for the control of doors and portals associated with a swing gate (i.e., a gate that can be used for both international and domestic flights). This requires special measures to ensure that the separation between domestic and international arrivals passenger traffic is maintained.

10.4 Trends

Perhaps the most dominant trend in airport access control is that the use of biometrics will likely become mandatory rather than voluntary. The capabilities of the various technologies have improved significantly in the last few years; 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 generally tend to be more inconvenient in the high-intensity airport operational environment. Nonetheless, they may be appropriate for certain limited applications such as cash operations, high-value storage, critical infrastructure locations, or certain types of tenant facilities, some of which may justify two-factor authentication. 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 still unanticipated 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.

10.5 Checklist

Access Control Systems Checklist

- ☐ Emergency Power/Battery Backup
  - All servers, field control panels, Operating stations, portal hardware
  - Credentialing system
- ☐ Data and Communications
  - Credential system
  - PACS server
  - Field controller to portal
  - Firewall—PACS to outside systems
- ☐ Duress/Convenience 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
  - Maintenance/personnel gates
  - Non-terminal AOA/SIDA doors

- ▪ Tenant and maintenance doors
- ▪ Tenant facility doors
- ▪ Navaids 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

SECTION 11: PERIMETER INTRUSION DETECTION SYSTEMS

11.1 Perimeter Issues

To delineate and adequately protect the AOA, SIDA, and other security areas from unauthorized access, the airport operator should assess the findings of risk and vulnerability assessments prepared for the airport, and whether natural barriers or other means of protection may be appropriate. Special attention should be given to areas where significant bodies of water are used as public recreational or fishing areas near the airport boundary. Access points for personnel and vehicles through the boundary lines, such as gates, doors, guard stations, and electronically controlled or monitored portals to/from the terminal and remote facilities, should also be considered.

The choice of an appropriate perimeter security system 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 Perimeter Intrusion Detection System (PIDS) is its ability to prevent unauthorized penetration; any access points through a boundary line should be able to differentiate between an authorized and an unauthorized user. At an airport, authorized access through boundary lines is constant and should happen in a timely manner to prevent unacceptable delays. 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 create the proper number of functional and maintainable access points that can benefit the airport.

Various boundary/barrier and access point types, as well as security measures that can enhance them, are described below. This information was derived from an industry-wide survey of airport technologies currently in use.

The most successful systems use multiple technologies, such as fence sensors or radars coupled with CCTV and/or thermal cameras; however, technologies alone are not likely to be fully effective unless integrated into the Security Operations Center (SOC) and backed by trained operators.

11.2 PIDS Requirements

PIDS serve as vital security countermeasures against physical security threats. A comprehensive PIDS monitors the exterior Secured Area and perimeter line (with or without barriers), detects surface intrusions into the area, alerts the security force of a detected intrusion, identifies the intrusion location, provides a means of intrusion assessment, and tracks both intruders and security personnel. (Interior security is addressed by other systems, although, in many cases, building security systems are integrated with the PIDS.)

A PIDS extends the physical sensing capability of the security force and significantly expands the defensive posture against physical security threats. Its objective is to provide the security forces with the capability to “See First, Understand First, Act First.” Keys to achieving this objective are the application of performance-based requirements, and integration of existing security systems with additional commercial-off-the-shelf security technologies necessary to realize mission success.

An effective PIDS provides modular scalable systems and equipment that can be assembled to protect assets varying in size from small general aviation airports to large commercial airports.

11.2.1 Intrusion Detection and Tracking

The intrusion detection and tracking function is concerned with detecting perimeter incursions, and once detected, tracking the intruders over designated airport areas. Proposed technical solutions should be evaluated in the initial Concept of Operations (ConOps) to determine an appropriate balance of user requirements.

The types of targets to be detected should be specified in the ConOps by the airport operator. These include people and vehicles, and for airports bordering bodies of water, boats, jet skis, and other types of watercraft. Low flying, low speed aircraft may also be detected by some technologies, although flocks of birds or unmanned aircraft systems (often called drones) may or may not be detectable, and thus, may or may not generate false alarms.

Detection technologies are sensitive to target physical size, e.g., height for video sensors and cross-sectional area for radars. The minimum cross-sectional area should be specified, which for detecting human and vehicle targets by radar is typically in the range of ½ to 1 square meter. Target speed should also be specified. For radar, this is typically in the range of 0.3 meters per second up to 36 meters per second; however, direction must also be specified, as some types of radars are direction sensitive.

Targets should be modeled as fluctuating, which means the physical dimensions or cross-sectional area presented to the sensor changes as the target moves. Similarly for cameras, the number of pixels on target must be increased to ensure a fluctuating target is detected. This, like radar, translates into a reduced usable detection range.

Intruder detection is usually performed in specified detection zones. These zones are usually near the perimeter and away from normal personnel and vehicular traffic. This is done to avoid the generation of target tracks associated with authorized personnel and vehicles. Each perimeter detection zone should be approximately 300 meters by 200 meters, or smaller, depending on the immediate environment.

The technology categories that are principally employed for intruder detection and tracking are: Video Motion Detection (VMD) and Tracking (VMDT); Ground Surveillance Radars (GSR); and linear-type perimeter sensors, such as fence sensors, infrared trip lines, and buried cables sensitive to seismic ground vibrations, which may be footsteps or seismic disturbances, or electromagnetic field disturbances.

GSRs have the advantage of covering large areas in both good and severe weather conditions. However, they lack a built-in assessment capability. In high clutter environments, such as found near gates or buildings, VMDT is preferred, as it provides a built-in assessment capability. The type of technology to employ is dependent on the airport environment. Typically, a combination of technologies offers the most cost effective solution to satisfy user requirements: GSRs along with long range pan-tilt-zoom (PTZ) cameras are used for large unobstructed areas; VMDT is employed in high clutter areas near terminals and other structures; and perimeter sensors can be used as an auxiliary means of detection in low traffic areas.

PIDS should combine detections of a target derived from multiple sensors into a single detection and generate a single track. This is critical to reducing operator workload.

11.2.2 Alarm Generation

Detection of an intrusion results in the possible generation of an alert or an alarm. Various approaches can be employed to determine if an alarm should be generated. For example, in a rule-based approach to alarm generation, the intruder track can be compared to a user defined map containing alarm boundaries. An alarm is raised if the track crosses a boundary. Other rules may include the direction and speed of travel. Alerts or alarms are then forwarded to the SOC for operator response action.

11.2.3 Intruder Classification and Tracking

A PIDS should be capable of making an initial automatic intruder classification that can be modified by the user. Target classes include persons, vehicles, animals, watercraft, and other types. A PIDS should be able to use target characteristics to make the initial classification. For example, any target located in a body of water is classified as a watercraft. Land targets above a certain speed, such as five meters per second, would initially be classified as a vehicle, while targets below this speed would initially be classified as persons.

A PIDS should be able to track targets with enough accuracy to direct response forces to the intruders. The PIDS should be capable of tracking targets that split (e.g., when intruders leave a vehicle), or targets that merge (e.g., when intruders enter a vehicle). A PIDS should also be capable of monitoring targets that stop, and then resume their motion within a reasonable period of time, on the order of several minutes. The maximum number of intruders the PIDS should be able to simultaneously track should also be specified by the airport operator.

Tracking of airport security force locations is essential for mounting an intrusion response. Security forces should be equipped with position locating and reporting devices—typically a GPS receiver and radio transmitter —to convey their positions and ancillary information to the SOC. The PIDS uses this information to distinguish intruder targets from security forces. Intruder and security force locations are typically shown on a facility map, each with different icons.

11.2.4 Performance Measures

A key parameter related to intrusion detection is the Probability of Detecting an intrusion (P_d). This should be specified by the airport operator for each type of sensor under the perceived local worst case scenario, including the effects of weather (rain, fog, etc.) Ideally, system P_d should be between 85 and 95 percent, and the system should be able to distinguish objects by class (persons, vehicles, or animals), and between serious and nuisance alarms. Each detection zone's P_d is calculated using scripted incursion scenarios. The results for each zone are then averaged and weighted by zone area to produce an overall system P_d. However, to avoid the possibility of a few very bad zones amid a large number of very good zones, a minimum zone P_d should be specified.

During the ConOps process of determining the most-cost effective solution, the airport operator should consider tradeoffs among sensors, and the ways different sensors may be used to compensate for weaknesses in any one sensor.

Assessing false alarm rates under different scenarios should be included in the tradeoff studies. A false alarm is generated internally by the sensor electronics or software. Radars typically have a low false alarm rate if properly sited without clutter in the radar beam path, which can block the beam and/or appear as false targets. VMD software and linear-type perimeter sensors are also site-dependent. It is important to test these technologies in the actual airport operating environment before selecting a vendor's product, as performance is quite often sensitive to the environment in which it is employed.

Suppliers should provide quantitative models and simulations of a PIDS's detection and tracking coverage, along with its P_d map in specified poor weather conditions to demonstrate analytically that its design satisfies the detection and tracking requirements laid out in the ConOps.

Another key performance measure is system response time. For integrated systems, this should be measured in seconds from the time an intrusion is made to when the intruder location is displayed on a facility map and assessment video is available for review. Shorter response time requirements generally result in a higher system cost.

11.3 Barriers and Detection Technologies

11.3.1 Natural Barriers and Physical 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 areas, and cliffs, etc.

When considering whether any natural barrier is an appropriate boundary, the airport operator should take into account the findings of the risk and vulnerability assessments prepared for the airport ConOps, 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 the stockpiling of earthen materials. 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.

Using time and distance from critical facilities to be protected is another deterrent factor. This concept suggests that if an unauthorized entry were to occur at a particular location, the amount of time and the distance covered combined with a high level of visibility would significantly reduce the likelihood of the intruder reaching the critical area without detection and/or intervention. Time and distance may be considered as an enhancement to standard physical barriers/boundaries when those boundaries are relatively removed from the critical areas they are protecting.

The security design principle known as "Detect, Delay, Respond" can be applied to the protection of a relatively remote perimeter or facility. The remote area may require only moderate boundary security measures if it is sufficiently removed from the primary security-related areas to allow the system time to detect an intrusion through use of technology, and delay the progress of the intruder until an appropriate security response can be implemented.

Physical barriers can be used to deter and delay the access of unauthorized persons into nonpublic areas of airports. These are usually permanent barriers designed to be an obvious visual barrier as well as a physical one. 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.

11.3.2 Fencing

Fencing is available in several designs that are difficult to climb or cut; or are provided with motion, tension, or other electronic sensing means. For fences with sensors, either mounted on the fencing or covering areas behind the fencing, there are other security system elements for monitoring the sensors and responding to intrusion alarms. Table 11-1 shows some of the available types of fence fabrics with American Iron and Steel Institute (AISI) and American Society for Testing and Materials (ASTM) ratings.

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 coils of stranded barbed wire on top, angled outward at a 45-degree incline from the airside. Fabrics should be secured to the fence posts and to the bottom rail 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. Fences configured in this manner are shown in Figure 11-1. Use of concrete mow strips below the fence line can deter tunneling underneath the fence by persons and animals. Mowing strips may also reduce maintenance hours and costs.

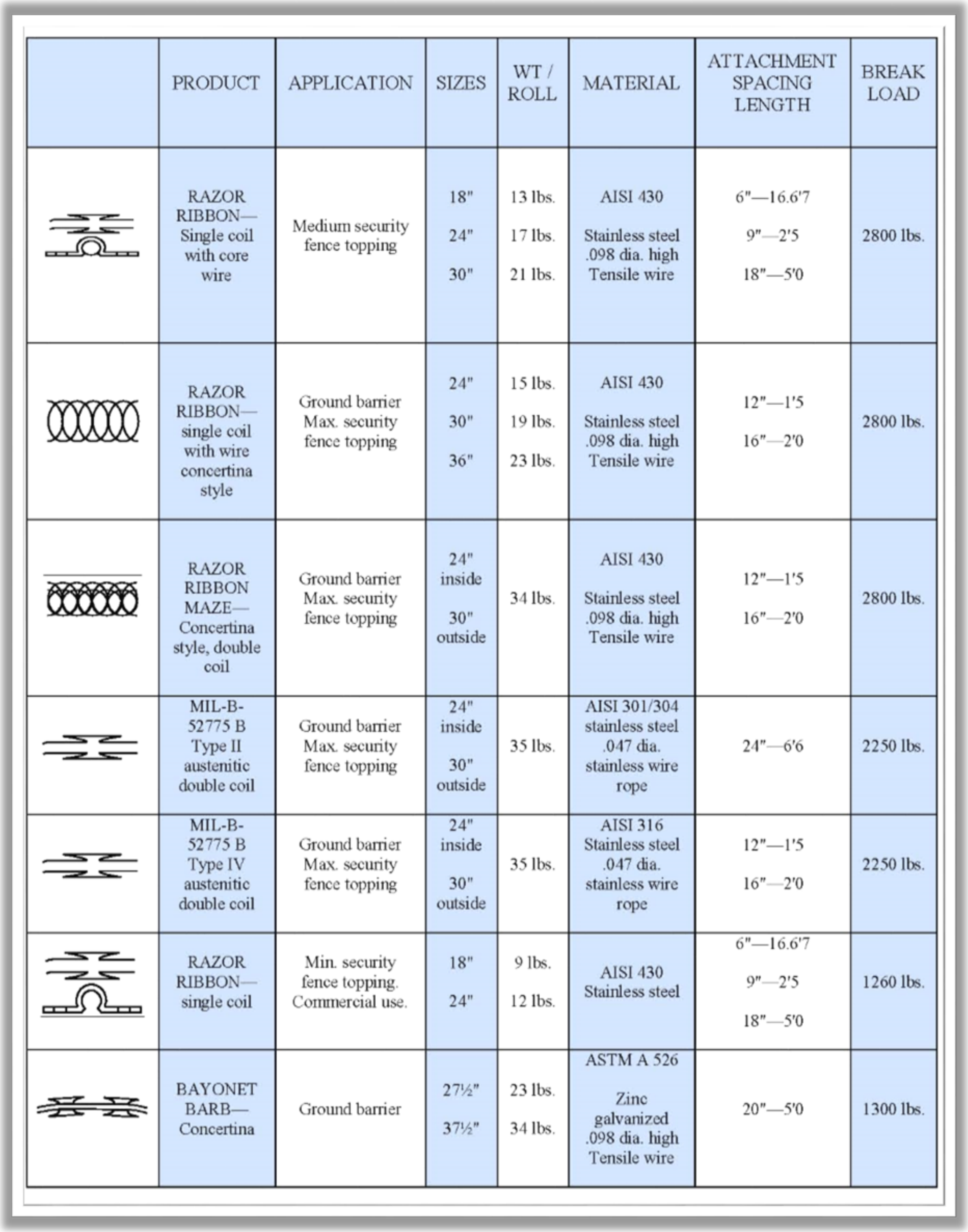
Chain link fencing is normally the most suitable and economical physical barrier for securing the airside, although this may vary somewhat with airport-specific conditions and topography. It is also readily available through a large variety of sources and is easily and inexpensively maintained. This 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 CCTV lines of sight and detection zones for various sensors.

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.

Table 11-1. Typical Chain Link Fence Barbed Wire Configurations

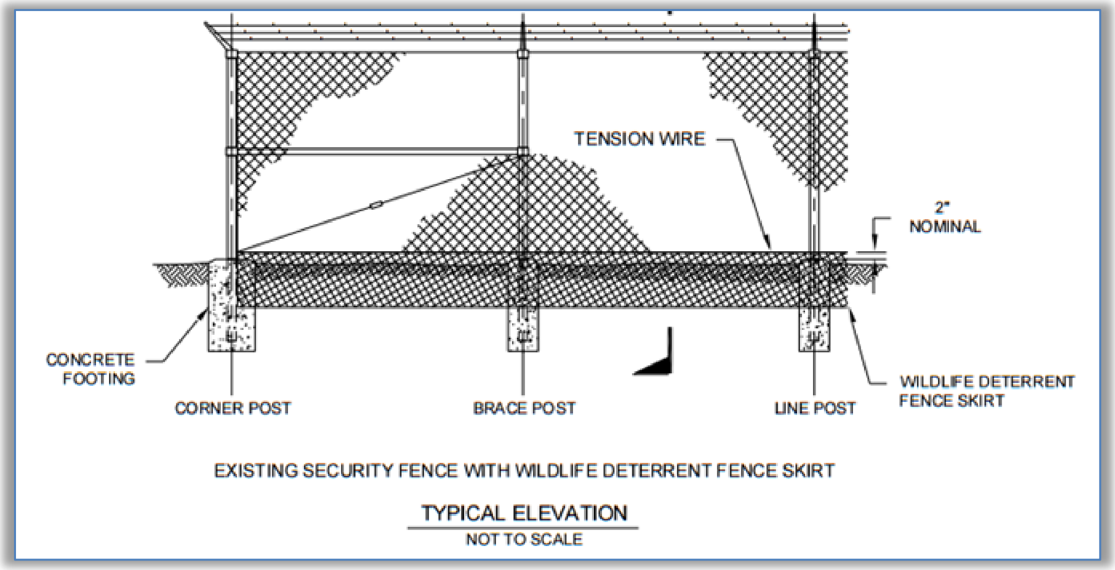


	PRODUCT	APPLICATION	SIZES	WT / ROLL	MATERIAL	ATTACHMENT SPACING LENGTH	BREAK LOAD
	RAZOR RIBBON—Single coil with core wire	Medium security fence topping	18" 24" 30"	13 lbs. 17 lbs. 21 lbs.	AISI 430 Stainless steel .098 dia. high Tensile wire	6"—16.6'7 9"—2'5 18"—5'0	2800 lbs.
	RAZOR RIBBON—single coil 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"—16.6'7 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: Chain Link Fence Manufacturers Institute

For safety or operational reasons (e.g., presence of navigational systems), some sections of perimeter fencing may not be able to meet standard security specifications. Special surveillance or detection measures may need to be applied to improve the safeguarding of these areas. In some cases, sections of non-reflective wood or plastic fencing may be appropriate.

Figure 11-1. Security Fence with Wildlife Deterrent Fence Skirt



Source: Chain Link Fence Manufacturers Institute

More specific information on fencing materials and installation, including the use of barbed wire outriggers, is available in FAA Advisory Circular 150/5360-13, *Planning and Design Guidelines for Airport Terminal Facilities*; and Advisory Circular 150/5370-10, *Standards for Specifying Construction of Airports*, among others.

Note: As this Guidelines document is being finalized, FAA has released a *draft* for industry comment reflecting many changes in AC 150/5360-13A, *Planning and Design for Airport Terminal Facilities*. When published, AC 150/5360-13A will cancel both AC 150/5360-13, and AC 150/5360-9, *Planning and Design Guidelines for Airport Terminal Facilities at Non-Hub Locations*.

In summary, fences are the most basic first line of deterrence and defense. Guidance is available from the Chain Link Fence Manufacturers Institute, including detailed technical and procurement specifications for security fencing.

11.3.3 Buildings and Walls

Buildings and other fixed structures may be used as a part of the physical perimeter barrier, and 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, or 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 separation. In addition, walls play an important part as visual barriers and deterrents.

11.3.3.1 Interior Walls

When interior walls are to be used as security barriers, consideration should be made to the type, construction material used, and their height. When possible, security walls should be full height, reaching not just suspended ceilings, but complete floor to ceiling or slab.

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.

11.3.3.2 Exterior Walls

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

Walls of solid materials 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. Blast 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.

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 Secured Area is maintained to at least the level maintained elsewhere along the boundary.

11.3.4 Access Points

Typically, there are numerous intended access points through fencing or other barriers for both vehicles and pedestrians. Access points through buildings or walls are usually doors; 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.

11.3.5 Gates

While the number of access points should be kept to a minimum, adequate pedestrian and vehicle access points must be allocated to support routine, maintenance, and emergency operations.

11.3.5.1 Routine Operations

Routine operational gates at an airport are typically those used by operations personnel, police patrols and response teams, catering, fuel and belly cargo vehicles and tugs, scheduled delivery vehicles, and ground service equipment and maintenance vehicles.

Most airport gates used for 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.

11.3.5.2 Maintenance Operations

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.

11.3.5.3 Emergency Operations

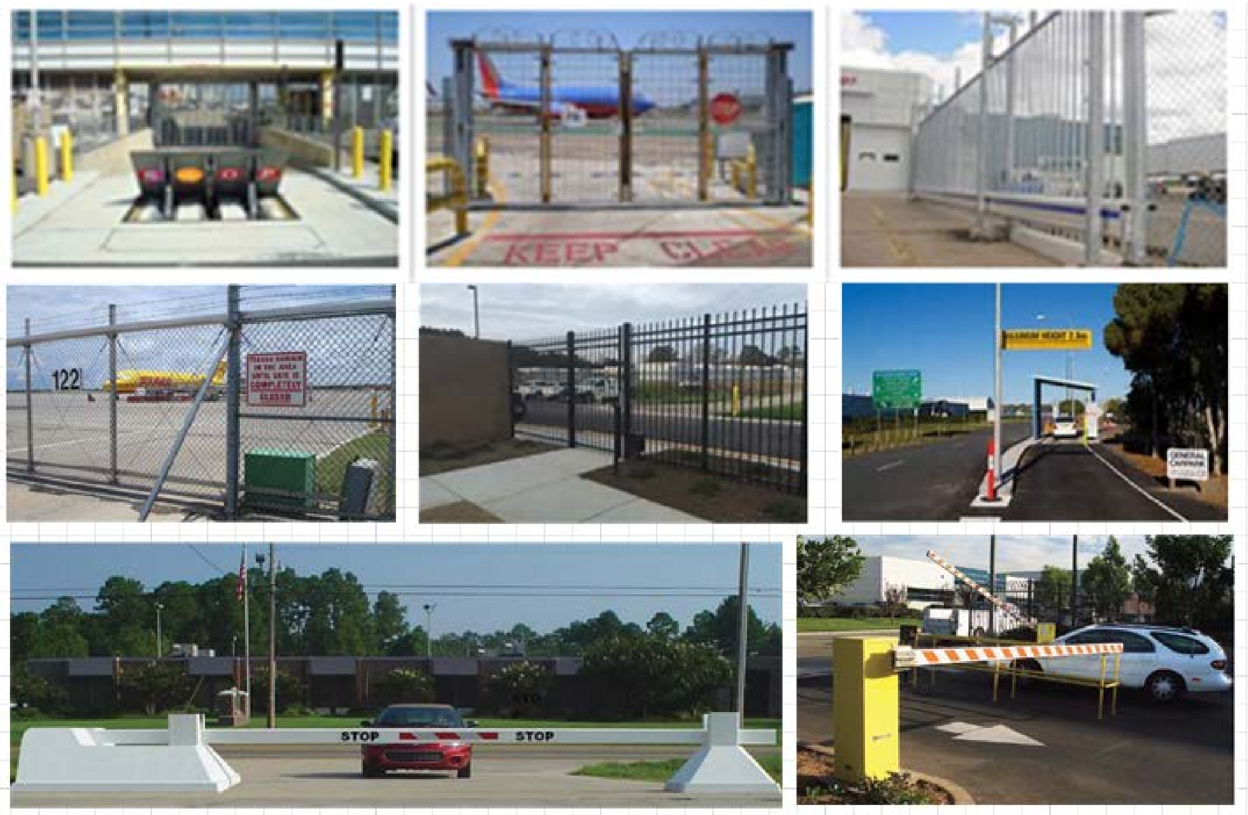
Emergency operations gates are used by on-airport and mutual aid emergency response vehicles responding to emergency situations, especially those involving an aircraft; these gates may also be used for regular operations.

Airport emergency operations gates may be controlled from an emergency operations center, or from the ARFF response vehicles themselves.

The capability for emergency response vehicles to crash through frangible mounts at emergency operations gates should be considered during the gate design, as should alarms on those gates. Special paint markings should be considered to identify the frangible fence or gate sections to approaching response vehicles. However, the decision to provide such frangible mounts and associated paint markings should be carefully evaluated against the findings of the risk assessment or vulnerability assessment prepared for the ConOps. While such crash gates and markings would help first responders during emergency situations, there is always the possibility that perpetrators could also utilize these gates to gain unauthorized access to the facility.

Gates are available in a variety of configurations and with specifications that can be tailored to local requirements, as illustrated in Figure 11-2.

Figure 11-2. Examples of Airport Gate Installations



Source: TranSecure, Inc.

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 required by enhanced security conditions. Swing gate hinges should be of the non-liftoff type or provided with additional welding to prevent the gates from being removed. Motor operator/controllers on gates should be located on the secure side of the gate. Battery/Uninterruptible Power Supply (UPS) backup power for the gate operator motor and security devices (card readers, CCTV, buried induction loops, intercom, and area security illumination/lighting) to allow a 2-hour gate open-close operation is essential to continuing vehicle traffic circulation during a power failure. Both the entry and exit gates should have UPS backup, as well as the security devices and the cameras to monitor any piggybacking by personnel.

Specifications based on the ConOps for operational gate requirement 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 as well as possible vehicle tracking measures.

Security provided by gates can be improved 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 phenomena, 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 be certain 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. CCTV may deter breaches at those facilities and may provide an improved response when breaches occur. Additionally, CCTV may provide a visual record that can be used to document breaches that become the subject of investigations. At unmanned gates, an open vehicle gate could be breached relatively easily by a pedestrian, so surveillance measures are preferred.

More specific information on gate materials and installation is available in FAA Advisory Circular 150/5360-13, *Planning and Design Guidelines for Airport Terminal Facilities*, and Advisory Circular 150/5370-10, *Standards for Specifying Construction of Airports*, among others.

11.3.5.4 Automatic Gates

In cases where gates are automated and induction loops are used on the airside of gates for free vehicle exit, the loop should be located to minimize the possibility of objects being thrown or pushed from the public side to activate it. Additional access control measures, such as microwave, infrared, other vehicle sensors, or CCTV monitoring may be desirable along with the loops when space is limited or more security is needed.

Access control devices (such as card readers or other monitors) serving exterior vehicle gates should be protected to reduce possible physical damage from passing vehicles. Properly placed curbing, bollards, and highway railings are useful. Equipment should be protected from weather, including extreme heat or cold, inside equipment enclosures, which can affect the operation of electronic and mechanical components. Heaters and/or fans are available as standard options for most access control devices, housings, and operators.

11.3.5.5 Doors with Access Controls

Numerous technologies are available for controlling access through doors, and there are many ways of implementing their use at any kind of doorway—wooden, glass, metal, single doors, double doors, and roll-up doors, as well as electronic barriers where there is no physical door at all. The designer should take into account any existing legacy systems the airport might wish to retain and integrate with new systems, and whether newer advances in technology might suggest a complete or partial replacement of the old systems to provide better security management. An extensive discussion of this issue is found in the RTCA document DO-230G, Security System Standard for Airport Access Control, which is also summarized in Section 10 of this document.

11.3.5.6 Sensor Line Gates

Sensor line gates and/or electronic gates function as typical access controlled gates, except that a sensor line (microwave, infrared, etc.) is used instead of a mechanical barrier. Depending on the sensor technology used (see Electronic Boundaries), these may be comparable in cost to mechanical ones.

The use of sensor line gates is typically feasible as a second, interior boundary where delays due to the mechanical operation of a physical gate are not practical, where space is limited, or where additional vehicle monitoring is desired. Sensor line gates are most often used to control vehicle access into a Secured Area or in cargo or maintenance areas where time is critical.

11.3.5.7 Automated Portals

Automated access portals are designed for high-throughput, performing access control in a high-speed, multi-user fashion, with a positive means of access denial of unauthorized persons, and with the capability of preventing access if multiple or unauthorized persons attempt to enter. Where these are employed, the delay induced by door opening/closing is eliminated. These portals are designed to replace high-throughput doors where piggybacking is a concern, or to add sensing technology to prevent contraband (explosives, drugs, or weapons) from entering high-throughput areas.

Video analytics technology can monitor the direction of the intruder’s movement and automatically provide photographs of security violators. As technology advances, the capability and affordability of automatic portals will increase and should be evaluated for high-throughput and/or special-use locations. See Section 12, Video Surveillance, for guidance on using video analytics.

11.3.5.8 Off-Airport Access Gates Including Crash Gates

Special perimeter gate construction applies for ARFF access to off-site areas in the event of an aircraft accident in an area adjacent to airport property. While the primary responsibility of airport-based firefighting units is to respond to aircraft emergencies that occur on the airport, in certain situations, to reach the accident site, ARFF units may have to use perimeter gates that are locked or require special procedures for opening/closing. Such gates are commonly called crash gates, and use frangible mounts; these provisions should be specifically included in the Airport Emergency Plan. The FAA also requires that ARFF training include operation of the various types of perimeter gates on the airport.

11.3.6 Exit Lanes

Securing exit lanes is addressed in Section 10, Access Control Systems.

An airport may still want to provide security measures such as video surveillance of approaches to an exit lane, especially if the exit is an exterior portal rather than to an area inside a terminal. There may also be situations where TSA will want to share such video for its own purposes, including post-event assessments.

11.3.7 Vehicle Inspection Stations, Road Barriers

Staffed vehicle inspection stations and vehicle crash barriers in roadways may be necessary in high-threat areas to control access in and around the airport terminal and other airport facilities. Non-permanent measures may also be necessary during elevated threat levels or in high-risk areas. This aspect of airport design should begin with the results of the vulnerability assessment undertaken during the planning phase.

The purpose of vehicle inspection stations is to provide a location outside of the blast envelope in which to inspect vehicles that are approaching the airport terminal on the public roadway. Vehicle inspection stations may also be necessary at parking locations within the blast envelope. The following features should be considered at vehicle inspection stations:

- Turnstiles, roll gates, or vehicular crash barriers should be provided that will stop or impede gate crashing.
- A sheltered checkpoint station is recommended. The shelter should be designed to permit maximum visibility over the immediate area of the station and to provide easy access for the guard to carry out the duties of inspecting vehicles and their contents. Security measures may include armored construction, shatter resistant glazing, video cameras covering approaches to the gate and for automatic license plate recognition, and both wired and wireless communications links to the SOC.
- Sufficient space should be considered to direct a vehicle to one side for further inspection without blocking access for subsequent vehicles. Dependable and instant communications from these stations to the SOC or other appropriate central location should be installed, maintained, and frequently tested. Sufficient space should be provided for emergency and other pre-authorized vehicles to bypass the vehicle inspection stations when necessary. A duress alarm should be provided.

11.3.7.1 Vehicle Barriers

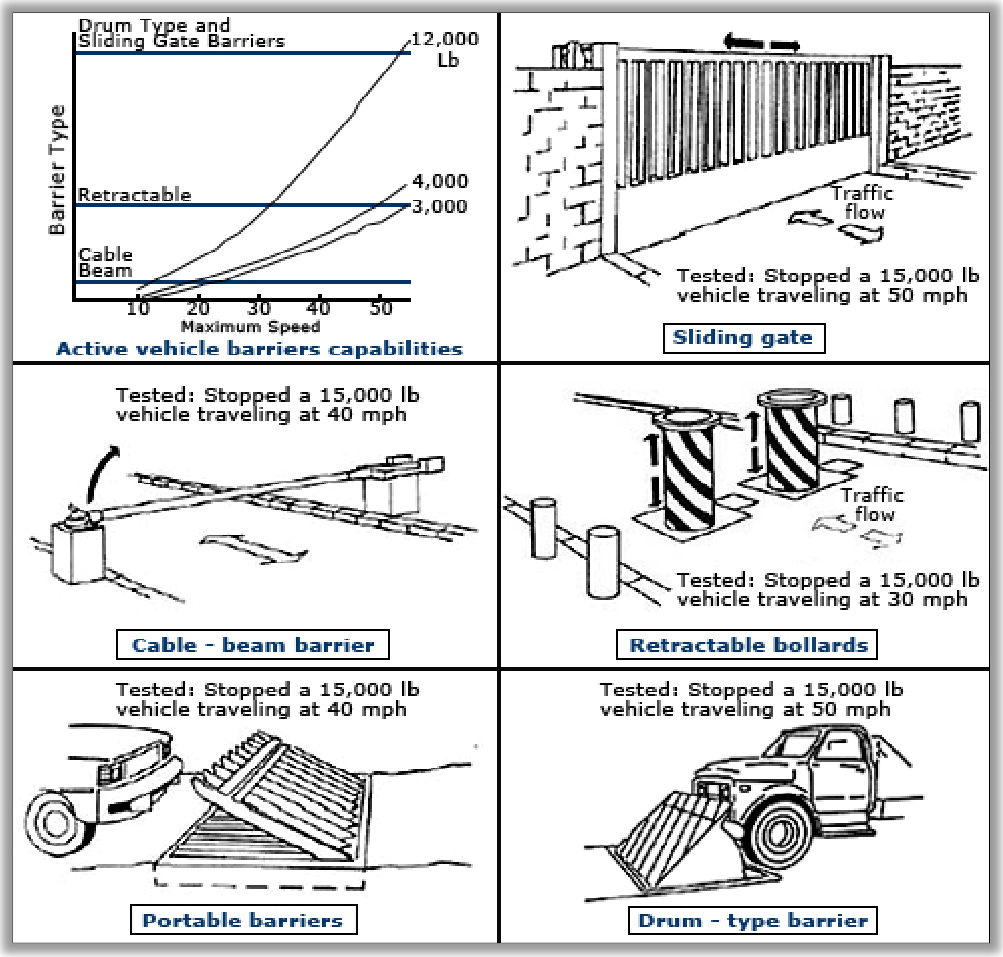
Ample vehicle queuing distance and vehicle inspection portals should be provided to avoid traffic backups and delays.

Airports are faced with the possibility of attack by explosives-laden vehicles, also known as Vehicle-Borne IEDs (VBIED).

There is a considerable body of knowledge on blast effects and protective measures available from U.S. government laboratories and agencies, under the auspices of the ASTM. This topic is addressed in more detail in Appendix B.

Figure 11-3 below illustrates the types of barriers that might be employed for various airport security applications, depending on the severity of the threat and the level of protection required. Complementary measures should be considered, such as physical setbacks of buildings and natural barriers or berms, when developing a blast protection solution. Table 11-2 displays the blast consequences radii for various types of threats, and the types of blast-protection measures that might be considered to protect against each type of threat.

Figure 11-3. Types of Road Barriers


Drum Type and
Sliding Gate Barriers
12,000
Lb
Barrier Type
Retractable
4,000
3,000
Cable
Beam
10
20
30
40
50
Maximum Speed
Active vehicle barriers capabilities
Traffic
flow
Tested: Stopped a 15,000 lb
vehicle traveling at 50 mph
Sliding gate
Tested: Stopped a 15,000 lb
vehicle traveling at 40 mph
Cable - beam barrier
Traffic
flow
Tested: Stopped a 15,000 lb
vehicle traveling at 30 mph
Retractable bollards
Tested: Stopped a 15,000 lb
vehicle traveling at 40 mph
Portable barriers
Tested: Stopped a 15,000 lb
vehicle traveling at 50 mph
Drum - type barrier

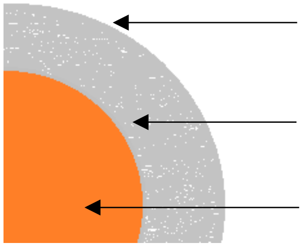
Source: U.S. Department of Defense Manual FM 101

Table 11-2. VBIED Explosion Hazard and Evacuation Distances

Bomb Threat Stand-Off Distances

This table is for general emergency planning only. A given building's vulnerability to an explosion depends on its construction and composition. The data in these tables may not accurately reflect these variables. Some risk will remain for any persons closer than the Outdoor Evacuation Distance.

	Explosives Capacity[1] (TNT Equivalent)	Mandatory Evacuation Distance[2]	Preferred Evacuation Distance[3]
 Pipe bomb	5 LBs 2.3 KG	70 FT 21 M	1,200 FT 388 M
 Suicide vest	20 LBs 9.2 KG	110 FT 34 M	1,750 FT 518 M
 Briefcase/suitcase bomb	50 LBs 23 KG	150 FT 46 M	1,850 FT 580 M
 Sedan	500 LBs 227 KG	320 FT 98 M	1,950 FT 580 M
 SUV/van	1,000 LBs 454 KG	400 FT 122 M	2,400 FT 732 M
 Small delivery truck	4,000 LBs 1,814 KG	640 FT 195 M	3,800 FT 1,159 M
 Container/tanker truck	10,000 LBs 4,538 KG	880 FT 263 M	5,100 FT 1,555
 Semi-trailer	60,000LBs 27,216 KG	1,570 FT 479 M	9,300 FT 2,835 M



Preferred Evacuation Distance
Preferred area (beyond this line) for evacuation of people in buildings and mandatory for people outdoors

Shelter-In-Place Zone
All personnel in this area should seek shelter inside a building away from the windows and exterior walls. Avoid having anyone outside – including those evacuating – in this area.[4]

Mandatory Evacuation Distance
All personnel must evacuate (both inside and outside of buildings)

[1] Based on maximum volume or weight of explosive (TNT equivalent) that reasonably fit in a suitcase or vehicle

[2] Governed by the ability of typical US commercial construction to resist severe damage or collapse following a blast. Performances can vary significantly, and buildings should be analyzed by qualified parties when possible.

[3] Governed by the greater of fragment throw distance or glass breakage/falling glass hazard distance. Note that pipe and briefcase bombs assume cased charges that throw fragments farther than vehicle bombs.

[4] A known terrorist tactic is to attract bystanders to windows, doorways or outside with gunfire, small bombs or other methods and then detonate a larger, more destructive device, significantly increasing human casualties.

Source: DHS

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. However, in 2009, the State Department stopped issuing such certification; testing and certification of perimeter barrier products is now carried out under ASTM F2656-15 *Standard Test Method for Vehicle*

Crash Testing of Perimeter Barriers. This ASTM 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 can be described in terms of the ASTM rating system as being equivalent to the following:

K4 = M30-P1

K8 = M40-P1

K12 = M50-P1

In the above ASTM rates, “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 a penetration less than 1 meter.

11.3.8 Other Physical Security Measures

11.3.8.1 Fence Clear Zones

Security effectiveness of perimeter fencing is materially improved by the provision of clear zones on both sides of the fence, typically 3–5 feet, particularly in the vicinity of the terminal and any other critical facilities. Such clearance areas facilitate surveillance and maintenance of fencing, and deny cover to vandals, trespassers, and contraband.

Within clear zones there should be no climbable objects, trees, or utility poles abutting the fence line, nor areas for stackable crates, pallets, storage containers, or other materials. Likewise, vehicles should be prevented from parking along the fence. In addition, landscaping within the clear zone should be minimized or eliminated to reduce potential hidden masking locations for persons, objects, fence damage, and vandalism.

It should be noted that security-related clear zones along perimeters or elsewhere, have no relationship with, and should not be confused with FAA-defined runway clear zones that are associated with aircraft approach slopes under FAR §151.9 and §77.27.

11.3.8.2 Locks

Advanced electronic lock and key technologies should be considered, as well as the time-honored deadbolt lock, built-in door handle lock, or padlock and metallic key to secure a portal. These methods are particularly suitable for those portals that are low-risk, low throughput, or significantly distant from the main areas of concern or from communications nodes to the central control station. Securing perimeter access portals through the use of locks necessarily involves procedural elements such as a key management system, and the inherent difficulties of recording usage at numerous locations and reissuing all keys when some are lost or stolen. An important consideration in choosing lock systems is total life-cycle cost.

11.3.8.3 Doors

To prevent unauthorized access to the airside, doors leading from the unsecured public areas of the terminal to the airside that are under visual control of authorized personnel should be limited to the operational minimum. Nevertheless, where they are necessary, electronic devices or closely controlled lock-and-key procedures may the best control for these doors, as well as card reader/pin pads, and recent advances in biometrics, to minimize labor costs and to be able to track personnel using specific doors to the AOA.

Unsupervised emergency exit doors providing egress from the terminal to the airside should be avoided if possible. If such doors are necessary for life safety/fire code compliance, they should be equipped with audio and visual alarms. Consider mounting a police-blue lens (to differentiate security from fire alarms), preferably located on both sides of the door, which can be monitored from a supervised location such as an airport SOC. Consider the possibility of CCTV cameras on both sides of certain high risk or high traffic doors. The use of frangible devices or covers over emergency exit activation bars deters misuse. Some codes allow for special locking arrangements for emergency exits that provide delays of up to 45 seconds, depending on local fire and life safety codes, as long as reasonable life safety is assured. Building codes establish specific performance requirements for doors with delayed egress hardware. Each airport operator should work with local fire and building code officials to determine the best systems allowable to accommodate both emergency and security needs.

Passenger gates, aircraft loading bridges, and other devices used for aircraft loading must be capable of being locked or otherwise secured to prevent unauthorized access to the airside and to parked aircraft.

11.3.8.4 Guard Stations

Staffed guard stations to control access into a security area are appropriate at some locations. They provide a point of entry at which personal identification can be established and persons and vehicles can be permitted to enter according to local vehicle search program requirements.

Devices such as turnstiles, roll gates, pop-up barriers, or a remotely operated drop-barrier gate may be used at guard stations to impede passage through the guard station until access authority is verified. In the case of vehicle access points, gates and barriers should provide the same or greater standard of security as any adjacent fencing to maintain the integrity of the area.

Use of a sheltered checkpoint station is recommended for gates staffed by security personnel. The shelter can be designed to permit maximum visibility over the immediate area of the gate and to provide access for the guard to carry out inspection of vehicles and their contents.

Sufficient space should be provided to direct a person or vehicle to one side for further inspection without blocking access for those following. Space should also be provided to allow vehicles refused entry to turn on the non-secure side and exit. Vehicle lanes and inspection stations should be provided in sufficient quantity to meet the expected traffic volumes, average inspection and processing times, and size of the largest vehicle entering the checkpoint. Stations may employ vehicle manifest pre-clearance checkpoints and special expedited clearance lanes for recognized deliveries. Dependable and instant communications from these stations to a central location must be installed, maintained, and frequently tested.

It is essential to provide communications between any sheltered security checkpoint station and the airport security services office, as well as to provide a duress alarm by which emergency assistance may be summoned.

In some applications, a vehicle access point may be remotely controlled by use of a card reader or similar credential verification device, in conjunction with CCTV monitoring taking place in the airport's SOC.

11.4 Electronic Boundaries and Technologies

Electronic sensors, motion detectors, infrared, or microwave sensors are clearly intended to serve the same security functions in protecting boundaries as other detectors but are simply employing different technologies, often with somewhat higher maintenance costs. Usually these applications will be used in conjunction with other reporting and assessment methods, such as alarms or CCTV. Nonetheless, there are appropriate places for using such applications, especially where normal conduit and cabling might be impractical, or where excessive trenching might be required.

While this document is focused on planning and design during the initial stages of current projects, new facilities such as terminals, cargo, or service facilities may sometimes take 4 or 5 years from the drawing board to processing the first users, aircraft, and passengers. When planning for a new terminal, and all other related facilities requiring a security perspective, one must take into account continuing developments throughout the airport industry, and the technologies that contribute to its secure wellbeing. While it may not be possible or even prudent to adopt first-generation beta-version technologies (although there may also be some corresponding advantages in such an approach), it is virtually certain that technology developments in many areas will afford new security capabilities and new requirements in the foreseeable future.

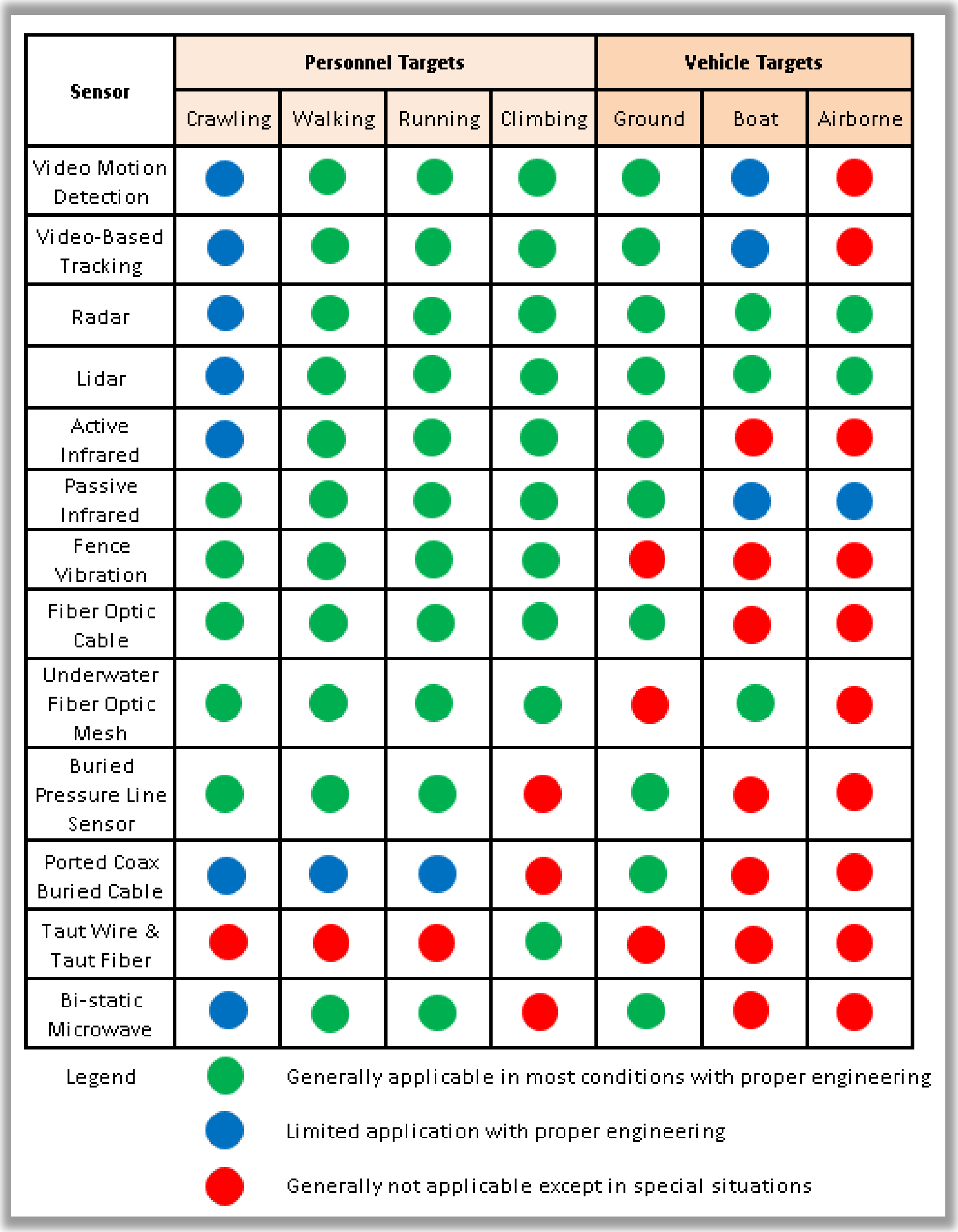
Among these is a rather broad concept called "data fusion," in which a wide array of sensors, surveillance techniques, data analysis, and communications capabilities and procedures are brought together to enhance the ability of airport security personnel to monitor and respond to a wide range of alarms. This includes the use of automated system analyses and alerts, thereby expanding an operator's vision and capability several fold.

Whether this is a necessary, immediate, or even desirable course of action for your airport, as new technology becomes tested and available, it may be useful and cost-effective to consider such expansion early on when designing infrastructure such as cabling to perimeter locations, power sources, lighting, and communications. By doing so, planners can avoid the need for costly actions such as re-trenching, replacing limited panels, or relocating camera positions.

A wide variety of exterior and interior sensor technologies can be selected to address the defined threats and/or vulnerabilities. In some instances, a combination of sensors may be deployed to achieve the desired level of detection while minimizing nuisance and false alarms.

Both exterior and interior technologies are noted below, with an emphasis on exterior technologies. The performance of each sensor technology is usually highly dependent on the local environment in which it is deployed. Extensive testing of potential sensor solutions should be performed by the airport operator on-site to ensure the appropriate sensor mix is effective. This testing should occur before final equipment approval is granted. Table 11-3 summarizes target classes for each detection technology and the types of motion each technology can most likely detect.

Table 11-3. Sensor Technology Detection Sensitivity



Sensor	Personnel Targets				Vehicle Targets		
	Crawling	Walking	Running	Climbing	Ground	Boat	Airborne
Video Motion Detection	🔵	🟢	🟢	🟢	🟢	🔵	🔴
Video-Based Tracking	🔵	🟢	🟢	🟢	🟢	🔵	🔴
Radar	🔵	🟢	🟢	🟢	🟢	🟢	🟢
Lidar	🔵	🟢	🟢	🟢	🟢	🟢	🟢
Active Infrared	🔵	🟢	🟢	🟢	🟢	🔴	🔴
Passive Infrared	🟢	🟢	🟢	🟢	🟢	🔵	🔵
Fence Vibration	🟢	🟢	🟢	🟢	🔴	🔴	🔴
Fiber Optic Cable	🟢	🟢	🟢	🟢	🟢	🔴	🔴
Underwater Fiber Optic Mesh	🟢	🟢	🟢	🟢	🔴	🟢	🔴
Buried Pressure Line Sensor	🟢	🟢	🟢	🔴	🟢	🔴	🔴
Ported Coax Buried Cable	🔵	🔵	🔵	🔴	🟢	🔴	🔴
Taut Wire & Taut Fiber	🔴	🔴	🔴	🟢	🔴	🔴	🔴
Bi-static Microwave	🔵	🟢	🟢	🔴	🟢	🔴	🔴

Legend
🟢 Generally applicable in most conditions with proper engineering
🔵 Limited application with proper engineering
🔴 Generally not applicable except in special situations

Source: TranSecure, Inc.

11.4.1 Intrusion Assessment

An operator performs an assessment using cameras upon detection of a potential intrusion to confirm intrusion detection, decide upon an appropriate response, and provide critical situational intelligence to a first responder team. Megapixel cameras and PTZ cameras are typically employed for intrusion assessment.

The system should display the associated alarm video immediately upon detection of an intrusion so the operator can assess the intrusion. Real-time video of intruders is preferred over recorded pre-alarm video. However, pre-alarm video may be useful in determining the circumstances under which an intrusion was initiated. Manual pre-alarm video retrieval should be provided so that an operator can see what generated the alarm, if the video is available. This pre-alarm video can play in a loop to assist the operator in assessment.

Substantial additional cameras may be needed to provide this pre-alarm video capability. The operator should have the capability to manually reclassify a target, based on assessment video, so that false or nuisance alarms may not require immediate response.

All alarm video, from detection and intrusion through resolution, should be recorded for later analysis and potential legal proceedings. This video should be watermarked to ensure no tampering has occurred.

11.4.1.1 Performance Measures

The key system parameter related to assessment is the ability to classify a target correctly. For video sensor performance metrics, see Section 12 of this document. Models of the assessment coverage should be provided to demonstrate that the design satisfies the assessment requirements in worst case weather conditions. Assessment coverage should be verified during the operational test phase.

11.4.1.2 Video Surveillance

Video surveillance cameras fall into three categories:

- Monochrome and color video (CCTV) cameras used in fair weather daylight conditions
- Low light level video cameras used at night where ambient lighting conditions are good
- Infrared cameras used for nighttime and poor weather conditions

Cameras are typically mounted in fixed positions, to cover specific areas, or on pan/tilt units to cover a range of areas and to follow moving targets. Where assessing target details is important, cameras will often have zoom lenses and variable focusing capabilities.

Cameras employ encoders that digitize the image for transmission over a communications network. For networked cameras, data transfer should be IP based.

The airport operator should specify several key camera requirements, including:

- Resolution, which is dependent on the functions the camera will perform. These include discriminating between target (e.g., person) and non-target objects (e.g., dog); classification (e.g., person, vehicle, watercraft); and identification (e.g., a particular person or vehicle type).
- Frame rate (e.g., 7.5, 15, or 30 frames per second [fps]), which affects the smoothness of the video. For most security surveillance operations, 15 fps is adequate for assessment applications, while 7.5 fps provides a useful assessment capability with lower communications bandwidth and storage requirements. When video analytics are employed, the frame rate should be at least 7.5 fps.
- Compression ratio (e.g., MPEG H.265 etc.), which reduces the amount of video data that is transmitted and stored. Compression allows more cameras to be deployed for a fixed or limited amount of bandwidth. Compression can be lossless, which means that the original video information can be perfectly recovered, or exhibit some loss, which means that some higher frequency information may be unrecoverable.

- Each of these factors affects the video storage required and communications bandwidth necessary to provide assessment. See Section 13 for additional information on Communications.

Tracking targets from camera video during an intrusion may be employed automatically or manually, depending on the video system design (derived from the ConOps). SOC operators should be able to assume manual control of any camera at any time. When in automatic camera tracking mode, the system should hand off the scene from one camera, as the target leaves its field of view, to a new camera whose field of view the target has entered.

How and where video cameras are positioned to secure a perimeter is a major design issue. If cameras are placed to look along a fence, their capabilities to sense and then track approaching intruders who breach the perimeter will be limited. Alternatives to be evaluated during the design process include:

- Placing cameras within the perimeter, looking outward
- Using dome cameras and/or cameras mounted on pan-tilt platforms
- Integrating video sensors with other PIDS components such as radars and fence sensors

11.4.2 Video Motion Detection

Video Motion Detection (VMD) algorithms apply analytical functions to assess changes in a scene over time. Detection ranges are determined by camera type, chip size, lens focal length, pole height, camera pitch, object size, and weather conditions. Thresholding is applied to limit false/nuisance alarms. Some systems are also capable of tracking an object as it moves in a camera’s field of view.

Video may be analyzed at the camera using an embedded analytics capability if a distributed architecture is desired, or at one or more analytics servers if a centralized architecture is employed. Each architecture has advantages and disadvantages, so the selected architecture will be dependent on the airport operator’s needs, as determined in the ConOps.

- Environmental Effects: Extreme weather (rain, snow, fog, and wind-blown debris), inconsistent (blooming) and low light levels, natural and man-made shadows, constantly changing background (such as blowing vegetation), obstructions, smoke or steam plumes, headlights at night, and uneven terrain can severely impact VMD performance.
- Assured Source of Electrical Power: Emergency power may be needed both for the cameras and the light sources to provide effective use both indoors and outdoors during a power failure.
- Target Characteristics: These include size, aspect, contrast, and reflectivity (or emissivity for infrared cameras). For example, clothing or left objects that match the background in very dark scenes is hard to detect.
- Response Time: The time needed to detect an intrusion is dependent on the object speed, size (i.e., the required number of pixels on target), and direction of motion (objects moving towards the camera rather than across the field of view take longer to detect). Activity at the extreme ends of the camera field of view impacts performance and the number of cameras required.
- P_d and False Alarm Rates: These rates are sensitive to the facility environment as well as to target characteristics.

- Area Coverage: Cameras are limited by the line-of-sight, and therefore are vulnerable to defeat by hostile forces concealing themselves behind impenetrable structures or objects such as buildings, trees, or terrain (e.g. hills).

Once a camera is positioned, problematic areas with constant motion or glare, and problematic times of day are going to be discovered during testing. Not every potential problem is relevant for every camera (for example, glare might be common in some camera positions and some times of day, but not in others). A set of standard perimeter intrusion scenarios should be conducted over a range of environmental conditions and target ranges. The following are relevant intruder behaviors that should be included in the testing:

- Typical penetration into the area, repeating with various people and different clothing
- Camouflaged penetrations: running, trying to be exposed as little as possible, slow-moving (e.g., crawling)
- Vehicle or watercraft penetrations where appropriate
- Camera tampering

11.4.3 Infrared (Thermal) Cameras

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 uses a sensor to convert the radiation into 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.

There are two types of infrared detectors: photon detectors and thermal detectors. Photon detectors usually offer better sensitivity and response times than thermal detectors. However, photon detectors require that the detector be cooled by liquid nitrogen or other means; therefore, they are larger, historically more expensive, and less reliable.

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 exhibit the same fundamental characteristics as video camera or video lenses, with selection still made by focal length, f-number (relative apertures), and cost.

Performance requirements should be established during the ConOps. 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 sense thermal signals through most window glass.

Video and thermal imagery fusion is another issue to be addressed in the ConOps. Imagery fusion is a process that is able to combine overlay images from a thermal camera with images from CCTV 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.

See Section 12, Video Surveillance, Detection, and Distribution Systems for additional information on thermal imagers and their applications.

11.4.4 Lighting Requirements

For CCTV cameras, lighting plays a significant part in intrusion detection, classification, and tracking. Security lighting, including infrared illumination, may not be possible in certain areas such as runways. Lighting also has value as a deterrent to individuals looking for an opportunity to commit a crime.

Normally, security lighting requires less intensity than lighting in work areas. At a minimum the designer should understand the different types that will support deterrence, human assessment, and CCTV assessment.

Existing or planned lighting should be considered when selecting camera models. Camera performance at night can be significantly impacted if camera sensitivity is not properly selected for ambient lighting levels.

Lighting of the area on both sides of gates and selected areas of fencing is highly recommended. Lighting can assure that fence/gate signage is readable, and that card readers, keypads, phones, intercoms, and/or other devices at the gate are visible and usable. Similarly, sufficient lighting is required for any area in which a CCTV camera is intended to monitor activity. Reduced lighting or sensor activated lighting may be considered for areas that have minimal traffic throughput in the off-peak hours.

See Section 12, Video Surveillance, Detection, and Distribution Systems for additional information on lighting and how it can be applied.

11.4.5 Non-Imaging Detection Technologies

11.4.5.1 Radar Systems

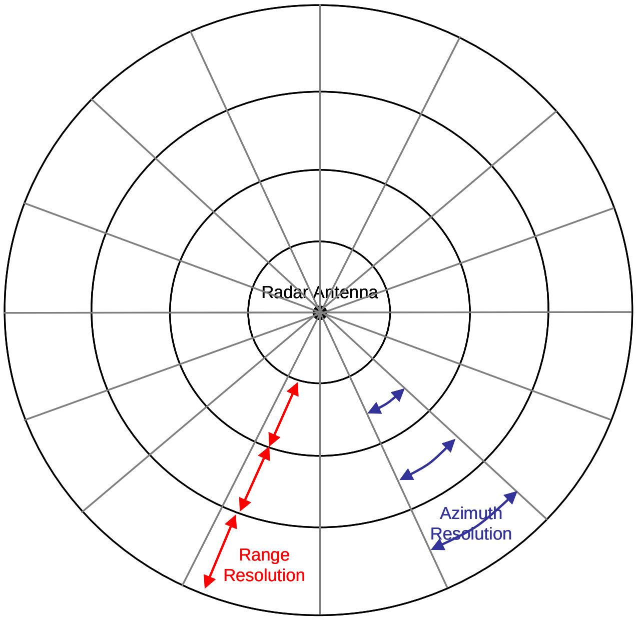
Radar systems are designed to provide volumetric area all-weather (in most cases) surveillance. Radar systems are able to search a wide area, detect and track an object, and provide accurate object location information, usually within seconds.

Generally, there are two primary types of radar systems for use in intrusion detection systems. These systems are defined by the methods each system employs to detect objects: (1) detection based on the movement of an object, known as Doppler radar; and (2) detection based on the amplitude or strength of the returned signal of an object, 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 would be an X-Band (~10GHz) system, with higher-band radars (35GHz and up) reserved for the specialized function 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. Both range and azimuth resolution are constant when measured in distance (e.g., meters) and angular (e.g., degrees) units, respectively. However, azimuth resolution, when converted to distance units, increases as the distance from the radar increases, as shown in Figure 11-4. Thus, range-azimuth cells farther from the radar are larger than cells closer to the radar. A narrower antenna beam width results in a higher resolution system.

Figure 11-4. Radar Resolution Cells



Source: US Navy

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.

Radar design issues include:

Type of Radar: Both pulse and Doppler radars are used for ground and marine surveillance. The choice depends on range, resolution, clutter rejection, cost, and other factors.

Performance: Range resolution is proportional to radar frequency (i.e., higher frequencies generally have higher resolutions), and are inversely proportional to environmental factors (e.g., higher frequencies are more easily absorbed by moisture in the air and to beam scattering by particles in the air). Designing for local environmental variables is an important aspect of predicting radar surveillance performance.

Line-of-Sight: Radars are linear beam detectors, and require clear fields of view to perform properly. Natural obstructions, terrain folds, and cultural clutter, such as buildings, impede radar beams.

PIDS radars should be high resolution in both range and azimuth to enable detection and tracking of closely-spaced targets. The PIDS designer should look for a radar system with a narrow azimuth beam width (such as 1 to 10 degrees) and a short pulse width (e.g., 100 nanoseconds). Doppler radars can also substantially improve the antenna beam width using a technique called beam-splitting that effectively narrows the beam by a factor of 10 or more.

Doppler radar systems are most sensitive to motion in the radial direction, and much less sensitive to motion in a transverse direction, which has low Doppler velocities. Non-Doppler radar systems suffer poor target discrimination when targets are in high clutter (unwanted return) areas, such as woods or buildings.

Radar systems can also be vulnerable to electromagnetic interference (EMI). EMI can be unintentional, such as interference caused by a navigational system at an airport, or intentional, which is known as jamming. Jamming is the purposeful transmission of electromagnetic signals with the intention of disrupting the performance of a radar system.

Radar systems detect; they may not perform target assessment and therefore they might be augmented with assessment cameras.

Implementation concerns focus on the use of multiple sensors in a cohesive fashion. Some radar sensors do not scan a full 360°, and many may rotate fully, but very slowly. In these cases, it is often advisable to deploy several sensors, each scanning an azimuth sector smaller than 360°, to cover a broad perimeter area. When deploying radar sensors in this fashion, it is desirable to allow the sensor scan sectors to overlap in order to form a more complete perimeter coverage pattern. If a target is in an overlap area, it will be detected by multiple sensors. The radar data processor must have a mechanism, such as a correlation function, to resolve multiple detections of a single target so that the system tracks and reports only one target.

11.4.5.2 Verify Radar Performance by Onsite Testing

Because of their sensitivity to site conditions and local environmental variables, a field survey should be conducted to geo-locate each proposed radar, and a sample of each candidate radar should be tested at each site to confirm coverage and detection performance.

Radar systems should be tested using targets moving at varying speeds (e.g., for humans, stationary, crawling, slow walking, walking, jogging, and running) through the different types of detection zones employed at the facility (e.g., smooth pavement, grassy fields, hilly areas, water areas, brush, or tall grassy areas) to characterize the system’s detection performance. Vehicles and watercraft targets should also be employed as appropriate to the facility.

11.4.5.3 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. Lidars can discriminate among targets based on object size. Lidars are sensitive to the same performance and environmental concerns as indicated for radars, including:

- Detection Capabilities: Lidar systems operate day and night, but they 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 in locations where surveillance is required.
- Extreme weather conditions will attenuate usable range. Particles in the air, such as smoke, smog, and fog can interfere with the sensor. Forested or densely urban areas are not well suited for lidar surveillance.
- Lidars can discriminate blowing rubbish and 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 therefore, should be augmented with assessment cameras.

As with radars, lidar systems should be tested in the airport environment using targets moving at varying speeds (e.g., for humans, stationary, crawling, slow walking, walking, jogging, and running) through the different types of detection zones employed at the facility (e.g., smooth pavement, grassy fields, hilly areas, water areas, brush, or tall grassy areas) may affect the system’s detection performance. Vehicles and watercraft targets should also be tested as appropriate to the facility.

11.4.5.4 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.

- Range: Up to 1,000 feet; varies with manufacturer
- Detection Capabilities: Walking, running, jumping, crawling, rolling
- Concerns: Fog, heavy rain, smoke, and wind-blown particulates will attenuate the beam. Tunneling, trenching, bridging, and climbing are problematic. Crawling under a detection zone or digging lose ground to tunnel under it, proximity to tall buildings or structures that would allow for easy jumping or bridging over, susceptible to animals and vegetation growth. If deep enough, snow may block the lower beams, giving no detection if someone crawls across in the snow.
- Types of Testing and Measurements: Walk, run, jump, roll and crawl through the detection zone. The most common defeat of this technology is vaulting over or crawling underneath transmission/detector units that are not secured by other means.

11.4.5.5 Passive Infrared Area Sensors

Changes in thermal radiation (i.e., temperature and target emissivity) due to objects passing through the sensor’s field of coverage can be used for intrusion detection.

- Range: 30–50 feet; varies by manufacturer
- Detection Capabilities: Walking and running
- Concerns: Targets at or near the ambient temperature are difficult to detect. Targets that avoid the coverage pattern cannot be detected. Targets that walk directly towards the sensor, rather than across the sensor’s field of view, are difficult to detect. Rapid temperature changes may cause false alarms.
- Types of Testing: Walking towards and away from the sensor, crossing the sensor field of view, slow moving targets, and entering sensor dead zones.

11.4.5.6 Fence Vibration Sensors

Fence mounted motion sensors can be used for intrusion detection by sensing fence vibrations associated with intrusion activities such as cutting or climbing, which are distinguished from normal vibrations.

- Range: Depends on the manufacturer.; a quarter-mile zone capability that can detect within 10 feet of the disturbance is typical
- Detection Capabilities: Cutting, climbing, or vibration and deflection of a sensor on fence
- Concerns: Tunneling, trenching, and bridging are problematic. May be susceptible to high false alarms from windblown debris, depending on sensitivity setting. Basic fence structure must be mechanically sound, stable, and well maintained.
- Types of Testing: Unaided climb, ladder climb, cutting, jumping, and fence panel lift

11.4.5.7 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 counter-clockwise 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 advantages of fiber optic sensors are freedom from EMI, wide bandwidth, compactness, geometric versatility, and economy. Fiber sensors are characterized by high sensitivity when compared to other types of sensors. They are also passive in nature due to their dielectric construction. Specially prepared fibers can withstand high temperature and other harsh environments. In telemetry and remote sensing applications, it is possible to use a segment of the fiber as a sensor gauge, while a long length of the same or another fiber can convey the sensed information to a remote station. Deployment of distributed and array sensors covering extensive structures and geographical locations is also feasible. Many signal processing devices (splitter, combiner, multiplexer, filter, or delay line) can also be made of fiber elements, thus enabling the realization of an all-fiber measuring system.
- Range : Single run cable can range 30 meters to several kilometers; zone lengths and maximum transmission distances vary with manufacturer
- Detection Capabilities: Cutting, climbing for fence and wall mounted fiber-optic cables; walking, running, jumping within the zone, crawling, trenching, and tunneling to some degree for buried fiber-optic cable
- Concerns: Bridging over or tunneling under the detection zone is problematic. Loose fence fabric, extreme temperature changes, and wind-blown debris may affect the sensor; if installed near runways, taxiways, roadways or train tracks that cause vibration, these effects may cause nuisance alarms; zone coverage should not be visually apparent
- Frozen ground and ground material variations are another concern. Buried fiber optic cables and other types of buried seismic sensors work well when shallow-buried in loose gravel, but other soils show dramatic sensitivity change when compacted or if water-saturated and subsequently frozen.
- Types of Testing: Walking, running, crawling, and climbing through the detection zone

11.4.5.8 Underwater Fiber-Optic Netting

Fiber optic cabling can be used to prevent and to detect underwater intrusions by configuring the optical cable into a mesh that covers entrances or perimeter approaches to facilities having a water boundary. The sensing phenomenon is the same as for surface optical cable sensing. The protective qualities of an underwater net depend on its strength, and for that reason, the optical cabling is usually embedded in a steel or synthetic polymer-strength member. When a breach occurs (i.e., the optical mesh is cut), the location of the breach is reported.

- Range: Based on extent of the netting
- Detection Capabilities: Any attempt to penetrate the net barrier (cut or tamper) will cause an alarm
- Concerns: Floating debris can cause nuisance alarms ; maintenance and repair costs are high; this is a relatively new technology, so long-term maintenance and life cycle issues are unknown; strengths and weaknesses for long term use have yet to be determined
- Types of Testing: Swimmers attempt to breach netting

11.4.5.9 Buried Line Sensor

Fluid-filled cable in plastic tubing can be used for intrusion detection. Usually, two tubes approximately four feet apart are used per detection zone. The tubes are very sensitive to pressure changes due to targets moving across the ground.

- Range: Typically about 100 to 1,000 feet
- Detection Capabilities: Walking, running, and crawling; vehicle and personnel intrusions are detected
- Concerns: Deep standing snow may attenuate the pressure signal caused by an intruder; nearby tree roots may transfer wind generated motion; animals may cause nuisance alarms; proximity to other sources of seismic energy may cause nuisance alarms; intruders moving slowly and employing cushioning may be difficult to detect
- Types of Testing: Persons walking, crawling, and running through the detection zone

11.4.5.10 Ported Coax Buried Cable

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

- Range: Continuous wave ported coax sensors use buried cables in multiple blocks, up to 500 feet each, and provide intruder location to the individual block. Newer 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 video assessment devices to detection areas of the perimeter, which may be obscured in other sensors such as tower-based radar or cameras. With the newer broadband systems, segments of the sensor cable can be electronically configured into multiple zones accessed from the central control station.
- Concerns: The area where the cables are run must be 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 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. Prescribed separation from vehicles on nearby roadways, or trains is required to avoid nuisance alarms, though the sensor is not vibration sensitive. Zone coverage with cables buried is covert and not visually apparent.
- Types of Testing: Walking, running, crawling, and jumping through the detection zone; segmenting of zones and zone boundaries (camera zones, sally ports, etc.) for broadband sensors

11.4.5.11 Taut Wire Sensors

- This system is a horizontal array of parallel, pre-tensioned barbed or barbless wires attached to sensors on a fixed sensor post to form a combined fence and sensor. It can also be installed on existing fences, walls, or roof edges. Taut wire systems are generally complex to install and maintain, but when properly installed, will exhibit low false alarm rates.

- Range: Segment lengths on either side of a sensor post are a maximum of 200 feet
- Detection Capabilities: The sensor responds to an intruder attempting to spread the wires, climb over them, cut them, or lean a ladder against the fence
- Concerns: Mechanical array requires regular maintenance to ensure wire tension consistency; metal wires are subject to expansion and contraction with variations in local temperatures and may require frequent adjustment; the system becomes more complicated if terrain is non-uniform or on a building mounting; tunneling, bridging, or compromising tension of wires must be addressed by other technology
- Types of Testing: Unaided climb, ladder climb, cutting, and spreading of wires
- Taut fiber sensors are similar in design, except they use fiber cabling rather than metal wire, which makes taut fiber immune to EMI and to changes in local temperature

11.4.5.12 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 that can cover long distances, depending on the unit. The detection field is invisible and fills the space between the transmitter and receiver. Stacking of units with different frequencies of operation or different polarizations can provide a higher P_d.

- Range: About 1,500 feet for X-band equipment, depending on the manufacturer
- Detection Capabilities: Walking, running, crawling, jumping, and rolling
- Concerns: 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 antennas not being detected; no standing water, which will cause false alarms; slow penetrations are problematic; limited by poorly defined detection patterns and nuisance alarms if large metal objects are nearby, or if windy conditions exist; proximity to similar high frequency radio frequency (RF) emitters will adversely affect the detection; fluorescent lights may also cause problems; interference can be avoided if narrow-band RF filters are used, as any jamming attempt should produce an alarm
- Types of Testing: Walking, running, crawling, and jumping through the detection zone

11.4.5.13 Other Technologies

Additional intrusion detection technologies include:

- Mechanical switches
- Magnetic switches
- Balanced magnetic switches
- Glass break
- Photoelectric beam
- Wall vibration
- Audio sensors

- Passive ultrasonics
- Active ultrasonics
- Electric field
- Capacitance sensors
- Strain sensitive cable
- Buried geophones

11.5 Trends

PIDS technologies are relatively mature but continue to improve and to be more effectively integrated into SOC operations with other security components, including access control and video surveillance units.

- Because of the wide variations among airport perimeters, and uncertainties regarding new measures that may be mandated by the Government, it is important that PIDS designs be flexible and adaptable.
- 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.
- Recent advances in economical, eye-safe, high power near-infrared diodes for commercial vehicle systems (autonomous driving and anti-collision functions) will make Lidar units increasingly attractive for beam and scanning PIDS applications. The trend to integrating video surveillance sensors and radars will increase in proportion to the availability of reliable, cost-effective radars.
- 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.

11.6 Checklists

PIDS

☐ Determine requirements per ConOps

☐ Physical Barriers:
- Align with security area boundaries
- Fencing
  - Based on vulnerability, cost
  - Typical: 7-foot chain link + 1-foot barbed wire
  - Motion, tension sensing available
  - Ground clearance 4-6 inches
  - In critical areas, anchor bottom
- Interior walls – full height, floor-to- ceiling
- Exterior walls – minimize hand holds

□ Natural Barriers
- Bodies of water; trees, dense foliage

□ Minimize Access Points
- Plan for maintenance, emergency ops
- Delivery and maintenance vehicles
- Electronic access points
  - Automatic gates, induction loop
  - Bollards to reduce vehicle damage
  - RTCA DO-230 access control standards

□ Electronic Perimeter Measures
- CCTV and thermal imagers
- Radar
- Buried line sensors
- Fence sensors – fiber optic and other types

□ Other Security Measures
- Clear zones, security lighting
- Consider life cycle costs, not just initial capital cost
- CCTV coverage
- TSA/FAA-required signage per /C 150/5360-12C
- Instructional/legal signage – per airport policy

Facilities, Areas and Geographical Placement Checklist

□ Facility Placement Considerations:
- Interaction among areas
- Types of activity in each area
- Flow of persons to/through areas
- Flow of delivery & maintenance traffic
- Need for security escorts

□ Each Airport is Unique

□ Facilities:
- Aircraft maintenance facilities
- Aircraft overnight parking area
- ARFF facilities
- SOC/CP
- Airport personnel offices
- Belly cargo facility
- Cargo area
- FAA ATCT and offices
- Fuel area
- GA areas
- GSEM facility
- GTSA
- Hotels and other accommodations
- Industrial/technology parks
- In-flight catering facility
- Intermodal transportation area
- Military facilities

- Navigation/communication equipment
- Rental car facilities
- State/government aircraft facilities
- Utilities and related equipment

SECTION 12: VIDEO SURVEILLANCE, DETECTION AND DISTRIBUTION SYSTEMS

12.1 Introduction

Airport planners and designers are continuously challenged by evolving video surveillance technology during lengthy design and construction projects. Every airport wants to operate with modern systems in place, but design and purchasing commitments must be made perhaps years earlier.

System and equipment specifications drafted during schematic design and development can be superseded by new technology and new standards by the time construction is completed, or during the projected life of newly installed equipment.

Planners and designers should systematically monitor technology trends that may impact their systems. They should also determine which near-term developments can be considered for their projects without jeopardizing project performance, schedule, and cost, while allowing for future enhancements.

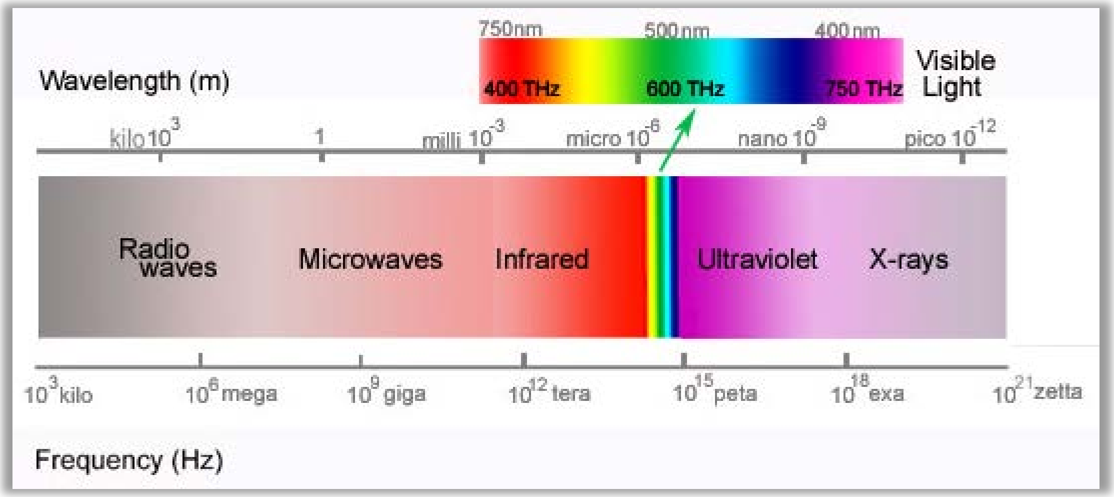
Nonetheless, airport security planning and design should be more concerned with the potential operational value added than with technical details such as software algorithms and the intricacies of each system's components.

12.2 Fundamentals

12.2.1 Imaging Spectrum

Video surveillance cameras operate in the visible and infrared sections of the electromagnetic spectrum. Figure 12-1 shows the range of frequencies used for imaging targets in these bands.

Figure 12-1. Visible and Infrared Imaging Bands



Source: US NIST

Visible light imagers, such as CCTV cameras, make use of light reflected from a target, including near-infrared wavelengths that are beyond the visual range of most persons. Infrared imagers sense energy at longer wavelengths of heat emitted from targets.

Imaging resolution is a function of wavelength. CCTV cameras will normally provide greater target detail than infrared imagers because of their shorter operating wavelengths. Visible light also penetrates glass (unless it has been treated), so CCTV cameras can "see" into buildings and automobiles.

Infrared imagers may provide less target detail, but because they process long wavelengths, they perform better in the presence of atmospheric obscurants such as fog and smoke, and this capability is independent of the presence of visible light. Figure 12-1 shows nominal atmospheric transmission at sea level under clear day conditions, with the infrared sensing bands superimposed. The band highlighted in green is the visible spectrum used by CCTV cameras. The longer wavelength infrared bands are highlighted in various shades of red; the energy must be detected by infrared sensors.

There are five options for imaging sensors to be considered in video surveillance:

- Visual band, by far the most commonly used and the most economical of the imaging options.
- Near-infrared (NIR) band, 0.75–1.4 µm (microns), used by image intensifiers and intensified CCTV arrays; also includes so-called bullet cameras and some laser pointers.
- Short-wavelength infrared (SWIR) band, 1.4–3 µm, which images energy gathered from the sky. This can be significant in urban areas and can improve sensor performance at night. SWIR sensors provide near-visual quality and can "see" through normal glass as well in light fog, but historically they have been expensive.
- Mid-wavelength infrared (MWIR) imagers operate in the 3–5 µm band, which is the band of choice when infrared target resolution is a priority. MWIR detectors may or may not use cryogenic cooling to improve their performance, the choice being driven by detection range and by sensor costs.
- Long-wavelength infrared (LWIR) imagers operate in the 8–15 µm band, which is the band of choice for imaging during poor weather conditions or in the presence of smoke. LWIR detectors also may or may not use cryogenic cooling to improve their performance, the choice being driven by detection range and by sensor costs.

12.2.2 Imager Performance Requirements

Development of a video surveillance strategy should begin during the ConOps, with an understanding of (a) the level of performance expected by the airport operator and the security staff, and (b) the technical and equipment options that can meet these requirements.

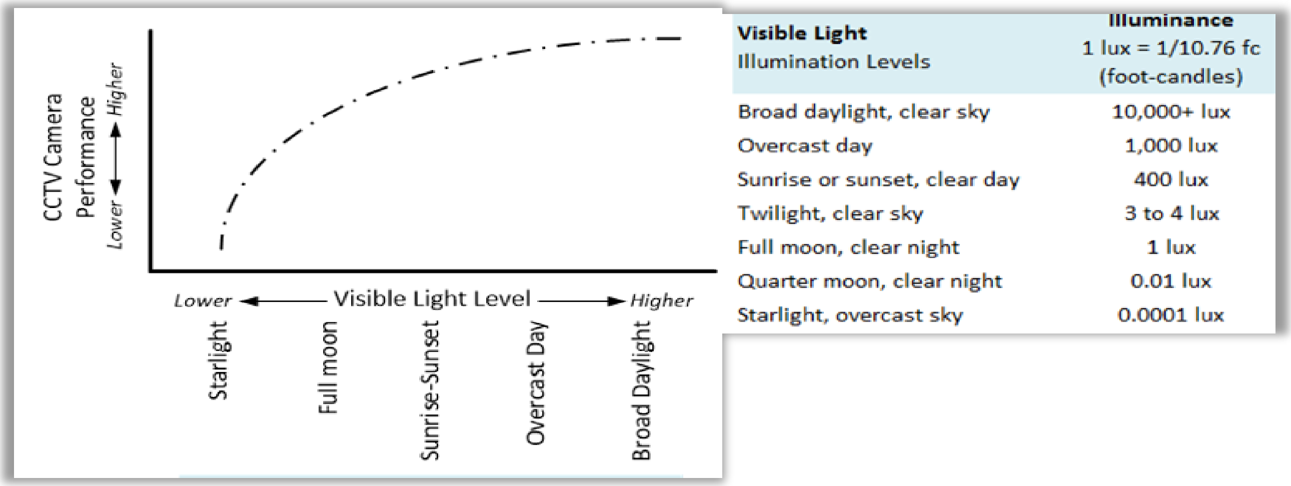
The performance of a surveillance system depends on a number of factors including:

- Characteristics of the object to be observed: Its dimensions, reflectivity, and contrast
- Local environmental conditions: Atmospheric transmittance (clear, foggy, snow) and turbulence; the level of scene illumination (expressed in footcandles or lux) and its variation over the 24-hour cycle; the type of artificial illumination (incandescent, metal halide, mercury vapor, sodium vapor, light emitting diodes (LED), etc.); how the cameras are situated with respect to that lighting, and the presence of strong light sources (street lamps and headlights) and glare in the scene; and movement of background (wind, trees)
- Camera characteristics: Detector size, sensitivity, signal-to-noise ratio, modulation transfer function, spatial resolution (in pixels and TV lines), and response to/suppression of bright lights in the scene

- Characteristics of the camera objective lens: Effective focal length (EFL), modulation transfer function, wavelengths for which the optics are corrected, and relative aperture (f/#)
- Characteristics of the display or monitor: Minimal spot size, resolution, contrast, and responsivity

The fall-off in performance for a typical camera detector as scene illumination is reduced is illustrated conceptually in Figure 12-2. The horizontal axis, scene illumination, is a logarithmic scale. There is a severe drop in camera array sensitivity at light levels below sunrise-sunset.

Figure 12-2. CCTV Camera Performance



Visible Light Illumination Levels	**Illuminance** 1 lux = 1/10.76 fc (foot-candles)
Broad daylight, clear sky	10,000+ lux
Overcast day	1,000 lux
Sunrise or sunset, clear day	400 lux
Twilight, clear sky	3 to 4 lux
Full moon, clear night	1 lux
Quarter moon, clear night	0.01 lux
Starlight, overcast sky	0.0001 lux

Source: TranSecure, Inc.

An example of the scientific approach for establishing operational performance requirements for camera-lens combinations are criteria developed by the U.S. Army Night Vision Laboratory, which tested the performance of night vision sensors and developed criteria for real-world imaging performance under field conditions. These models are being continually updated, but fundamental performance criteria have not changed.

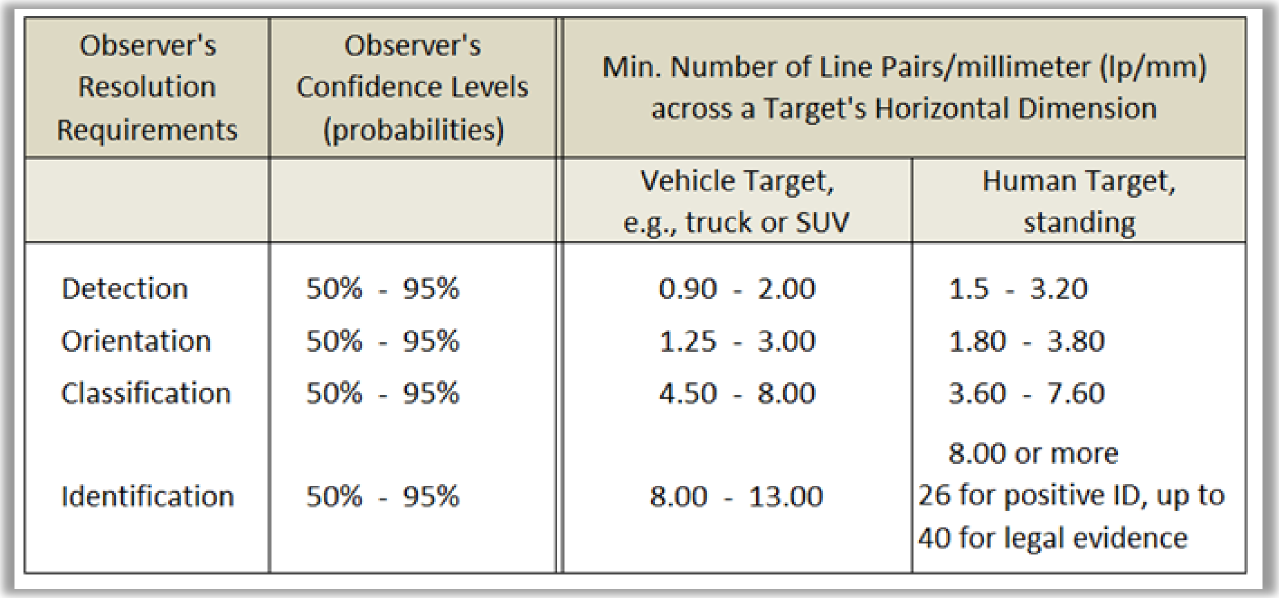
The Army criteria describe imaging performance in terms of the information needed at each of four levels of performance:

- Detection: The object is present, even if its features cannot be distinguished
- Orientation: The primary axis of the target (vertical for persons, horizontal for vehicles or large animals) can be sensed
- Classification: The class of target can be discerned, i.e., a person can be differentiated from an animal, or it can be discriminated whether a human is male or female
- Identification: Target characteristics within a class can be determined, e.g., a person can be recognized based on facial features and other characteristics

Table 12-1 highlights the increasing amount of information (resolution) required to move from detection to identification. The table includes two levels of confidence (probabilities) along with performance ranges for each level for vehicle and human targets.

Table 12-1. Resolution per Minimum Target Dimension in Line-Pairs

(1 line pair = 2 pixels; 2 pixels = 1 TV line)



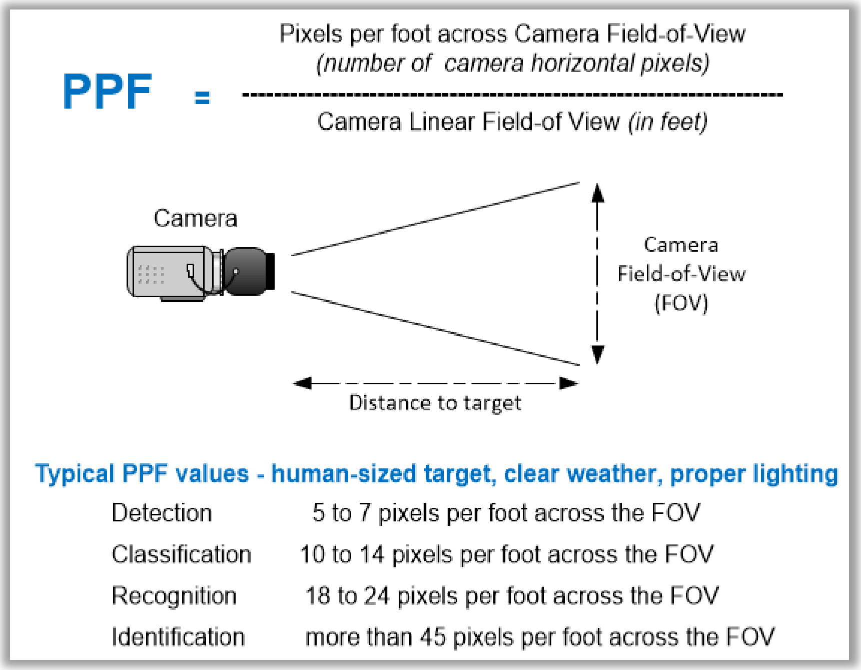
Observer's Resolution Requirements	Observer's Confidence Levels (probabilities)	Min. Number of Line Pairs/millimeter (lp/mm) across a Target's Horizontal Dimension	
		Vehicle Target, e.g., truck or SUV	Human Target, standing
Detection	50% - 95%	0.90 - 2.00	1.5 - 3.20
Orientation	50% - 95%	1.25 - 3.00	1.80 - 3.80
Classification	50% - 95%	4.50 - 8.00	3.60 - 7.60
Identification	50% - 95%	8.00 - 13.00	8.00 or more 26 for positive ID, up to 40 for legal evidence

Source: TranSecure, Inc. from U.S. Army data

If airport surveillance requirements are drafted using the above terminology, the parties designing the security system will be in a position to specify the proper equipment and the airport operator can evaluate the proposed design in operational terms.

To facilitate camera performance calculations, security integrators and camera vendors have developed a simple metric, known as Pixels per Foot (PPF). As Figure 12-3 shows, this is a geometric function in which the PPF metric is calculated from scene dimensions and camera detector properties (array size). PPF is a dimensional metric only; it does not account for variations in target characteristics or sensor performance.

Figure 12-3. PPF Metric for Measuring CCTV Camera Performance



PPF = Pixels per foot across Camera Field-of-View *(number of camera horizontal pixels)* / Camera Linear Field-of View *(in feet)*

Typical PPF values - human-sized target, clear weather, proper lighting

Detection	5 to 7 pixels per foot across the FOV
Classification	10 to 14 pixels per foot across the FOV
Recognition	18 to 24 pixels per foot across the FOV
Identification	more than 45 pixels per foot across the FOV

Source: TranSecure, Inc.

Suppliers recognize the usefulness of PPF values for setting objective performance standards that can later be used for acceptance testing. Several camera manufacturers now post recommended PPF values on their websites, and use these values in their proposals. The values are still subjective, and unless airport security personnel mandate different values, the manufacturer values are likely to become the basis for accepting installed cameras. Airport security designers should be aware of such websites and be prepared to deal with the values shown on them in negotiating camera performance requirements. These manufacturer websites are illustrative only, and do not constitute an endorsement of their recommended PPF values.

There is no similar metric available for infrared sensors; however, because of their longer wavelengths, infrared sensors are primarily detection devices with limited resolution for target classification or identification.

Camera selection should also include compatibility with other elements of a video surveillance system, particularly video management software (VMS) and video storage equipment, and, for extensively integrated systems, access control and other security functions. Equipment manufacturers have set up standards bodies for compatibility testing and to provide common grounds for specifying equipment functions. Two of these bodies, ONVIF (Open Network Video Interface Forum) and PSIA (Physical Security Interoperability Alliance) have published standards and testing procedures that have continued to evolve and gain acceptance with manufacturers, many of which now include ONVIF and/or PSIA compatibility in their specifications and on their datasheets. The extent to which such compatibility applies, and does not apply, for specific hardware and software is still for an airport operator to determine. The best way to do this is to set up a testbed in which candidate devices can be operated end-to-end to confirm compatibility.

12.2.3 Camera and Display Standards

The resolution and frame rates for U.S. and European video standards are shown in Table 12-2.

Table 12-2. Horizontal/Vertical Resolution of US/European Video Standard

		BCCD/CMOS Array		**Depth** **256 colors**	**Video Rate**
Standard	Resolution	H Pixel	BV Pixel	Bits	Frame/Sec
USA	VGA	640	480	8	30
NTSC/	QCIF	176	112	8	30
RS 170	CIF	352	240	8	30
	4CIF	704	480	8	30
	RGB	768	480	8	30
Europe	VGA	720	576	8	25
PAL	QCIF	176	144	8	25
	CIF	352	288	8	25
	4CIF	704	576	8	25
	RGB	768	580	8	25

Source: TranSecure, Inc.

For streaming video, the applicable network standard is the widely-accepted Real Time Streaming Protocol. For networked video, both wired and wireless transmissions of video are governed by the IEEE 802 series of Ethernet standards, which are updated from time to time.

In an analog video environment, once a video standard had been adopted (e.g., PAL or NTSC) the user had reason to expect that plugging into matrix switches and Digital Video Recorders (DVR) would enable video to be viewed without problems. The video standard, however, did not solve the problems of controlling cameras and lenses, because the control protocols were not standardized.

As of yet there are no accepted industry standards for interfacing digital video cameras to video analytics or to other elements of an integrated security system, including access control equipment and video storage.

Camera and display performance should be compatible; there is no point in specifying a high level of camera resolution unless the specifications for display enable this information to be shown to the operator in the Security Operations Center (SOC). Performance for cameras and displays should also be based on well-established standards (see Table 12-3).

Table 12-3. Camera and Display Resolution Standards

Camera Resolution		Display Resolution	
Camera Format by Array Pixels	Detector Pixel Count (HxV)	Display Format	Displayed Pixel Count (HxV)
SD / 0.3 MP	US 640 x 480 PAL 768 x 576	QCIF	176 x 144
		QSIF	166 x 120
720p / 1 MP	1280 x 720	SIF	320 x 240
2 MP	1920 x 1080	CIF	352 x 288
3 MP	2048 x 1536	4CIF NTSC	704 x 480 (D1) 640 x 480 (VGA)
5 MP	2592 x 1944		
		4CIF PAL	704 x 576
		16CIF	1408 x 1152

Source: TranSecure, Inc

12.3 CCTV Systems

CCTV surveillance systems have proven their worth for facility security over a period of more than 40 years. The equipment is relatively inexpensive compared to other means of surveillance, provides detailed images of scenes for positive assessment of what is happening in a familiar video presentation, and operates for years with minimal maintenance. CCTV systems are used to monitor a variety of activities and areas, including:

- Area surveillance in terminals
- Roadway approaches
- Curbside traffic
- Cargo loading docks
- Tenant access points
- Baggage handling areas
- Access to SIDA, AOA, etc.
- Monitor passenger/SIDA activity
- Gate activities
- Fenced perimeters
- Vehicle traffic control
- Rental car facilities
- Fuel farm areas
- Parking garage/lot monitoring
- Employee parking areas

12.3.1 CCTV Camera Properties

Previously, detectors in most surveillance cameras used tube technology. Modern surveillance cameras use solid-state detectors, primarily charge-coupled devices (CCD) but with an increasing use of complementary metal-oxide semiconductor (CMOS) arrays.

CCDs generally have greater sensitivity than CMOS arrays, which is an advantage for surveillance under the low scene illumination often found at airport perimeters. Compared to CCDs, CMOS arrays offer a higher pixel density, a broader dynamic light range, use less power, and are potentially less expensive because they can be fabricated with technology developed for personal computers. CMOS technology dominates megapixel (MP) camera detectors for these reasons.

Camera variants include analog video, which uses coaxial cabling, and IP cameras, which use IT networking cable. Each type has its pros and cons. Analog cameras are generally considered legacy types and provide standard definition performance equivalent to Super Video Graphics Array (SVGA). However, large Asian camera vendors have recently introduced a high definition line of analog cameras, known as HDTV, which are priced below IP megapixel cameras. HDTV cameras can provide the equivalent of 1 MP performance over coaxial cabling. For small airport video surveillance systems where coaxial cabling is already installed, this can result in significant cost savings in cable plant costs as well as camera costs. Networking such cameras is limited, as are intelligent video options, and each vendor has its own proprietary design, which locks out other vendors for storage and other accessories.

Camera performance is a function of scene illumination, how that camera is positioned and mounted to view the scene, and target properties. Scene illumination is especially critical at night. Visual-band cameras sense reflective light; the amount of reflected light depends on natural illumination, often augmented by artificial lighting, and the contrast and reflectivity of targets. Dark areas, such as asphalt parking lots, have reflectivity as low as 0.05 (5 percent). If the ambient light at the darkest point in a parking lot is 0.01 foot candle (fc), for a reflectivity of 0.05, a camera will sense only 0.0005 fc of the reflected light.

For very low-light conditions, CCDs and CMOS arrays can be fitted with image intensifier modules to operate down to starlight scene illumination levels. Intensifiers can significantly increase acquisition costs and also reduce operational life of the camera. Adding supplemental visible lighting to permit the use of normal CCD/CMOS cameras should be considered as a cost-effective alternative to using intensified cameras. Another alternative is the use of thermal imaging (infrared) cameras.

Detector size, and the horizontal dimension of the detector in particular, plus the focal length of the camera's objective lens, determine the surveillance field coverage of a camera and the distance at which an object can be imaged. Array cost is primarily a function of the number of good arrays a manufacturer can realize from a silicon wafer (i.e., the yield factor). Cost is generally proportionate to yield (number of good chips per silicon wafer), and this favors the smaller array sizes. As a result, most surveillance cameras use 1/4-inand 1/3-in arrays, especially dome cameras where compact size is important.

Camera detector size and lens focal length selection should be determined by what is to be viewed, at what distance, and with what resolution. In some instances, the angular or horizontal coverage of the camera will drive the design, especially for outdoor area coverage. In other cases, the ability to resolve target details will set the requirement.

Selection can also be limited by physical space availability, e.g., dome camera dimensions are more restrictive than box camera housings.

For cameras equipped with zoom objective lenses, magnification is often given as a combination of both optical zoom and electronic zoom. Increasing the focal length of a zoom lens will result in more "information" from the target being focused on the detector. Increasing the apparent magnification electronically, however, simply increases the size of the pixels and adds no new "information" about the target, so it is not a substitute for optical zooming.

Video surveillance cameras should be sited for overlapping coverage to the extent practicable, to protect against any camera failing and also to provide alternate views of objects to enhance their detection and tracking. The extent of overlapping coverage can readily be determined from a web-based camera-lens calculator and shown diagrammatically. Table 12-4 shows how horizontal, angular, and linear field coverage varies with detector size for a sampling of objective lens focal lengths. Coverage is a function of detector width and lens focal length.

Table 12-4. Horizontal Angular and Linear Field Coverage of Surveillance Cameras

	CCD/CMOS Camera Arrays				
Camera size	**1/4-in**	**1/3-in**	**1/2-in**	**2/3-in**	**1-in**
Detector width	**3.2 mm**	**4.8 mm**	**6.4 mm**	**8.8 mm**	**12.8 mm**
Lens Focal Length (mm)	**Horizontal Angular Field of View (degrees)**				
5	5.5	51.3	65.2	82.7	104.0
10	18.2	27.0	35.5	47.5	65.2
25	7.3	11.0	14.6	20.0	28.7
50	3.7	5.5	7.3	10.1	14.6
75	2.4	3.7	5.0	6.7	9.8
100	1.8	2.7	3.7	5.0	7.3
200	0.9	1.4	1.8	2.5	3.7
300	0.6	0.9	1.2	1.7	2.4
500	0.4	0.6	0.7	1.0	1.5
1000	0.2	0.3	0.4	0.5	0.7
Lens Focal Length (mm)	**Linear Field Average at 1000 Feet**				
5	640.0	960.0	1280.0	1760.0	2560.0
10	320.0	480.0	640.0	880.0	1280.0
25	128.0	192.0	256.0	352.0	512.0
50	64.0	96.0	128.0	176.0	256.0
75	42.7	64.0	85.3	117.3	170.7
100	32.0	48.0	64.0	88.0	128.0
200	16.0	24.0	32.0	44.0	64.0
300	10.7	16.0	21.3	29.3	42.7
500	6.4	9.6	12.8	17.6	25.6
1000	3.2	4.8	6.4	8.8	12.8

Source: TranSecure, Inc.

For airport operations, the operationally significant parameters of a CCD/CMOS camera include:

- Detector array size: CCD/CMOS arrays are available in different sizes, as the above table shows. The size of the detector, and most often its width (horizontal dimension) will determine angular and linear field coverage that can be achieved with a given objective lens.
- Effective picture elements (pixels): The number of horizontal pixels times the number of vertical pixels in a scene.
- Minimum resolution: The smallest division to which a measurement can be determined, generally expressed as TV lines.
- Sensitivity: A measure of the minimum change in an input signal that an instrument can detect. Camera sensitivity defines the minimum amount of light required to realize the camera's performance, and this relationship is not linear, i.e., a relatively small change in light reaching the camera detector can result in a much greater loss in camera performance.
- Many cameras are now equipped to clip, or attenuate, illumination spikes in the scene so that imagery is maintained as a camera is panned or when cars appear in the scene with headlights pointed at the cameras. Where such illumination spikes are likely to occur, airport security in the ConOps requirements should advise the surveillance system designer of such conditions.
- Some color cameras now change automatically to monochrome operation, in order to maximize resolution, when a low-light illumination threshold is reached.
- Dynamic range: The ratio of the full-scale range of a data converter to the smallest difference the detector can resolve. Dynamic range is generally expressed in decibels. Operationally, for airport security, it will be important to have sufficient dynamic range to operate from minimum illumination, such as street lamps at night, to full sun conditions. In high sun environments, this may require the use of neutral density filters in the lens to avoid saturating the camera detector if the maximum illumination cannot be controlled by a mechanical iris.
- Signal-to-noise ratio: The ratio of total signal to electronic noise expressed in decibels (dB).
- Minimum scene illumination: For a given lens f/#, the minimum amount of scene illumination required to produce an image at full video bandwidth.
- Backlight compensation: The dynamic range available to prevent a backlit subject from darkening an image or saturating the detector. This parameter is important when strong point light sources are present in the scene.

In most cases, a camera can be used inside a facility as well as outdoors, with the difference in configuration being the type of housing required for the particular environment. Lighting is also a factor. Light levels indoors generally vary over a small range, whereas outdoor conditions may vary widely over the day-night cycle depending on the extent of auxiliary lighting used. Where camera design requirements converge, designers should consider using the same cameras indoors and outdoors to simplify training and maintenance and to minimize replacement costs.

Indoor environmental conditions are generally under the airport operator's control. In most instances, special environmental conditioning should not be necessary. Housings still may be required to protect cameras from accidental or deliberate damage, even to the extent of armoring cameras against weapon attacks, and all such housings should include locks.

Exterior (outdoor) cameras will be subject to local temperature, wind, rain, and snow. They may also be installed on poles or sides of buildings where access is difficult. Cameras that are externally mounted may be susceptible to environmental elements such as moisture and wind-induced motion. These issues need to be addressed in the design phase.

To enable such cameras to operate reliably, it is advisable to install them in environmental enclosures, which, depending on local conditions, may include internal heaters, cooling devices, windshield wipers, sunshades, etc. The security system design should address these issues, and also address how maintenance is to be performed.

12.3.2 IP Cameras

IP cameras are network-ready imaging appliances. Depending on the operational requirements of the surveillance system, IP cameras can simplify the network infrastructure by enabling video, controlling signals for PTZ units, and transmitting electrical power over the Ethernet cable plant, thereby saving the expense of installing separate power and control cabling.

In an IP camera, the video signal is digitized internally and compressed for transmission over the network. Storage may also be embedded in the camera to reduce transmission bandwidth use.

The IEEE Power-over-Ethernet standard defines the means of powering IP devices over Ethernet cabling. The 802.3 standard enables 30 to 60 watts of power to be delivered to devices in this manner. This assumes that the IT network is already installed or expensed; that it has sufficient bandwidth for the number of cameras to be put on the network; that it has adequate performance quality (latency, jitter, and dropped packets) and security; and that network nodes exist at or in proximity to the IP camera. If a separate IT network is to be installed for the security system, then that cost should be factored into the system design tradeoffs during schematic design.

Many dome cameras and other types that use 1/4-in and 1/3-in CCD arrays are available as IP cameras. Few 1/2-in format cameras are available as IP cameras, and this situation is not expected to change. Megapixel cameras are generally IP cameras, and mostly use CMOS detectors because of yield and cost issues.

Installing and/or transitioning to IP cameras can be challenging. There are, as yet, no agreed-upon standards, and implementations differ among manufacturers with regard to video streaming, configuration, status notification, and other features. An installation plan, supported by a system acceptance test plan, is essential to realizing the desired system performance objectives.

12.3.3 Megapixel CCTV Cameras

Megapixel (MP) refers to IP cameras having arrays with a minimum of 1 million pixels. At the present time, this includes cameras with up to 33 million pixels.

The arguments for MP cameras are:

- High resolution: The increased pixel count gives much better quality image for both forensic and legal purposes; there is little benefit to capturing a criminal in the act if the resolution does not enable identification of the criminal.
- PTZ Alternative: A single fixed MP camera equipped with a wide angle lens, or with a motorized zoom lens, may be able to monitor large outdoor areas, such as parking lots, or long

indoor terminal concourses, which otherwise would require multiple fixed cameras. An MP camera can do this because the video image can be zoomed electronically, by three times or more depending on the pixel count, and still yield acceptable image quality on the user's monitor. With some MP cameras, electronic zooming also enables an image-within-an image to be created in real time. A user can designate an area of interest in the field of view and magnify an object within that area while still viewing the entire field coverage in the background, thereby retaining situational awareness across the area under surveillance. Zooming in on an object with a PTZ camera, by contrast, narrows the field coverage and carries a corresponding loss of situational awareness.

- Reduced Costs: Using a few MP cameras instead of a larger number of conventional cameras can reduce system acquisition and support costs.

The improvement in performance and reduced pricing have made MP cameras with 1 to 3 MP the new baseline standard for specifying video surveillance cameras. Performance improvements include better dynamic range (ability to work in high traffic areas that have different lighting levels, such as exterior doorways) and better low-light sensitivity. In these two functions, as well in unit pricing, 1 to 3 MP cameras are now competitive with standard definition cameras. MP cameras now afford designers opportunities for video surveillance that were previously not cost effective.

Operationally, a potential user should be aware of the following issues when considering MP cameras.

- The current offerings of MP cameras vary widely from manufacturer to manufacturer with respect to array size (number of pixels), software enhancements (such as image-within-an image), and compatibility with third-party equipment such as elements of VMS and analytics software—factors that complicate the selection and integration process.
- While often cost-effective for area surveillance, especially when maintaining situational awareness is important or when forensic-quality imagery is required, MP cameras are generally not cost effective for basic tasks such as monitoring doorways or low risk, low traffic areas.
- A larger number of pixels does not guarantee a large amount of detail. Some operational conditions will result in much less detail than would be expected by the pixel specifications, particularly when a camera is operating under less than ideal conditions, such as poor lighting.
- Current models of megapixel cameras generally do not perform well under low-light conditions, or in the presence of very bright lights. Expectations of a reduction in camera count may not be realized if night illumination is inadequate, thereby reducing field coverage and/or target distance. Where night surveillance is required, MP camera performance can be enhanced by upgrading a lighting system, which may be less expensive than using alternative imagers such as intensified CCTV cameras or thermal (infrared) imagers.
- MP cameras require higher quality, more expensive objective lenses than conventional cameras because of their small pixel dimensions. For large format MP cameras, including 1-inch arrays, the range of MP-qualified lenses is currently limited, and installing a lens designed for a smaller format will crop the image.
- The range of third-party video analytics for MP cameras, independent of the camera manufacturer, is limited at the present time.
- Image bandwidth varies widely even across cameras in the same model family, depending on coding and compression protocols and lighting conditions, with many cameras exhibiting bandwidth spikes at night in the presence of headlights and other strong light sources.

- Even with H.264 and H.265 video compression, storage requirements for MP cameras will be much greater than for conventional cameras.
- In the absence of agreed-upon industry standards, MP cameras pose the risk for a user to be locked into a proprietary, single-source solution.

MP cameras offer advantages for specific situations, and should be considered in that context rather than as a universal solution to every application. The additional marginal cost of MP cameras in locations that require them may be small compared with the total cost of ownership of the CCTV system over its expected life.

In some cases, a single, very large capacity MP camera may be able to cover a wide area. MP cameras are now available with arrays up to 33 MP. There are, however, disadvantages to relying on a single camera, including cost and the creation of a single-point-of-failure in the surveillance system unless dual units are installed. During Basis of Design trade studies, designers should compare this solution with using multiple, smaller MP cameras (e.g., 6 to 8 MP) regarding area coverage and installed cost, including the cost of VMS licenses and network cabling of the cameras.

12.3.4 Wide Angle IP Cameras

IP cameras capable of hemispherical and panoramic coverage are now available, which is in part the result of advances in MP arrays and objective lenses. The most common configuration is a dome, which may contain several cameras aimed for the desired coverage, or a single camera, which is rotated with the images and then “stitched” for a continuous output display.

Using wide angle IP cameras enables both wide area coverage, with short focal lenses, as well as the capability to electronically zoom in on a target for greater detail.

There are several applications where airports can leverage such technologies to reduce camera counts (and costs) while still providing necessary coverage. Examples include:

- Intersections of concourses, where a single panoramic camera can view all approaches as well as the intersection area
- Screening checkpoint approaches
- Baggage carousels, for overhead coverage as well as to surveil surrounding areas
- Exterior gates and portals where wide angular surveillance coverage is necessary on both sides of the secured perimeter
- Road intersections
- Cargo loading areas

Given the different offerings of camera manufacturers, testing on site and under actual operating conditions is critical to utilizing wide angle cameras. Testing should include:

- Area coverage and the identification of any blind spots; the adequacy of image detail for recognizing and/or identifying typical targets at ranges of interest
- How image quality is impacted by changes in lighting conditions
- Transmission bandwidth, which can spike strongly at night with point light sources and which will impact video storage requirements

- Frame rate compatibility with SOC viewing and with any analytical functions to be employed
- Compatibility with VMS and/or Physical Security Information Management (PSIM) software

The number and cost of VMS (or PSIM) and analytic software licenses (multi-camera units may require multiple camera licenses and multiple analytic licenses).

12.3.5 CCTV Camera Lenses

Camera lens types can be classified as:

- Fixed focal length lenses: The lens is manufactured to a specified focal length selected for the particular application.
- Varifocal lenses: The focal length of a lens can be adjusted manually over a specific range—e.g., between 25 and 100 mm—to tailor its coverage to the scene to be monitored.
- Zoom lenses: A zoom lens is a varifocal type in which the EFL of the lens, which determines scene magnification, can be varied. The zoom function is usually motorized for remote operation, along with pan-tilt functions. Some CCTV lenses are capable of zooming 20 to 30 times, which suggests long range performance. However, when a lens is zoomed, its relative aperture (f/#) changes proportionally. This impacts the light gathering capability of the lens and the performance of the camera array. At maximum zoom, the camera-lens combination may only provide useful performance during periods of broad daylight. Actual performance should be verified on site, over a full 24-hour period, before such lenses are specified.

For airport security operations, the lens parameters to consider include:

- EFL expressed in millimeters (mm): EFL determines the angular field of view (degrees) and linear field coverage (feet or meters) and viewing magnification.
- Relative aperture, commonly known as the f-number (f/#), which is the ratio of lens EFL to the diameter of its clear aperture. Relative aperture is the measure of lens light-gathering capability. It is especially important for viewing under overcast or low-light conditions. Doubling the numerical aperture, from f/2 to f/4, for example, will halve the amount of light transmitted by the lens to the camera detector, which can easily impact camera performance.
- For zoom lenses, the f/# is normally stated at the minimum EFL setting, e.g., f/1.4 at 25 mm. As EFL increases, so will the numerical f/#. Zooming a lens from 25 mm to 100 mm, for example, will increase the numerical aperture from f/1.4 to f/5.6, significantly reducing the amount of light gathered, to the point where a camera may not function under poor lighting.
- Optical correction: Not all lenses are equal, and lens quality should be carefully considered when using MP cameras, which have smaller pixel dimensions than conventional camera arrays.

MP cameras should be fitted with lenses specifically designed for MP arrays; otherwise, performance of the camera-lens combination may not be fully achieved.

CCTV cameras can also be fitted with active infrared light emitting diodes (LED) for supplemental illumination of dark areas, such as alleyways and perimeter areas sheltered from ambient light by foliage. These cameras are known as bullet cameras and also as integrated infrared cameras. The LEDs are selected for near-infrared operation at wavelengths of 0.85 to 0.9 microns, which is not visible to most persons. Typical configurations are shown in Figure 12-4; these cameras are generally used for target illumination at short ranges.

Figure 12-4. Typical Bullet Cameras

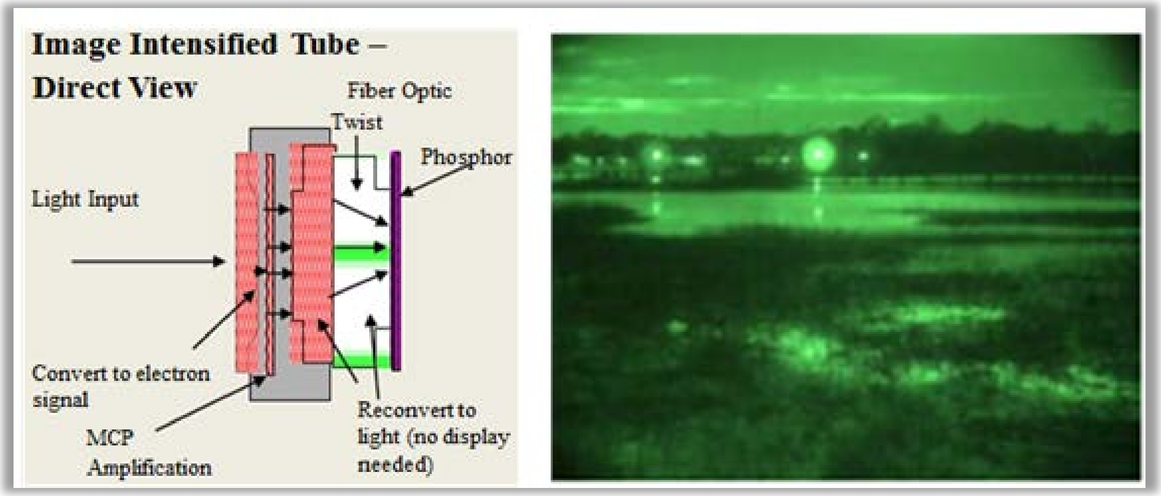
Source: TranSecure, Inc.

12.4 Image Intensified Sensors

Image intensification technology, also known as night vision technology, was developed by the U.S. Army during the 1960s to enable its forces to operate at night. The technology exploits weak ambient illumination, such as moonlight and starlight. The weak ambient illumination is collected by an objective lens, imaged onto a photodetector, amplified electronically (the gain mechanism), and displayed on a phosphor. When the phosphor output is viewed by an operator, it is known as direct view mode. When the phosphor is viewed by a video sensor, it is known as indirect view mode.

The technology is illustrated in Figure 12-5 for a direct-mode device, showing the components of an intensifier tube and the characteristically green color of the output phosphor.

Figure 12-5. Direct View Image Intensifier Tube and Output Presentation



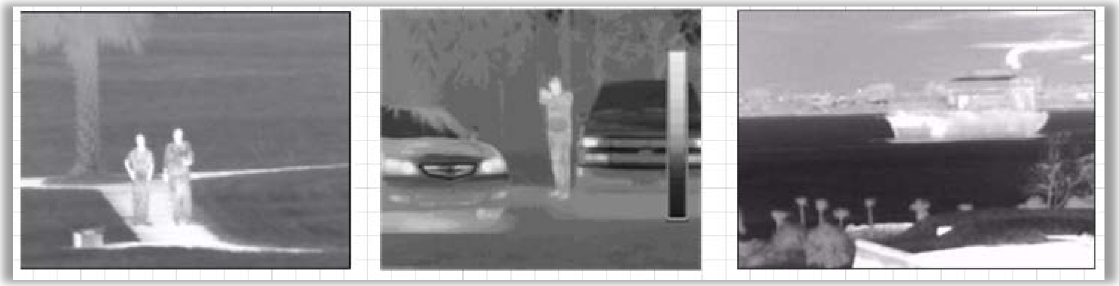
Source: U.S. Army

Until the availability of thermal imaging devices, intensified video cameras were the only practical means of performing surveillance at night. Bullet cameras, which are inexpensive, and thermal imagers, especially less costly uncooled imagers, have largely replaced intensified video cameras in physical security applications, except when an operator must carry an imager and remain mobile.

12.5 Thermal Imaging (Infrared) Sensors

Thermal imaging sensors, also known as Forward-Looking Infrared (FLIR) sensors, sense heat emitted by targets and do not depend on visible (reflected) illumination. This means that day and night performance can be nearly the same. Because they operate at wavelengths longer than visible light, infrared sensors can often detect targets in modest fog and in the presence of smoke and heavy rain. Examples of infrared sensor presentations are shown in Figure 12-6.

Figure 12-6. Typical Infrared Imager Presentations



Source: U.S. Navy

Compared to visible CCTV imagers, infrared imagers have less resolution and are significantly more expensive than CCD and CMOS video detectors. Infrared imager optics are similarly more expensive than video camera lenses, and the selection of focal lengths is more limited. It may not be affordable to realize comparable range performance with FLIRs and video cameras, and this must be evaluated when considering the use of infrared imagers.

FLIR detectors are available with or without cryogenic cooling, which improves its performance, but is costly; in addition, the operational reliability of cryogenic coolers is limited. For airports, in situations where detection ranges are modest, uncooled detectors are the preferred choice.

Thermal imagers are most often used for outdoor surveillance under conditions where the level of visible light illumination and/or poor weather will significantly degrade the performance of visible CCTV cameras, involving a trade-off between performance and price; cooled detectors offer better performance, but are costlier because of their cryogenic coolers, whereas the less costly uncooled detectors may require larger and more expensive optics. Conventional glass optics block infrared energy, which is why thermal imagers cannot see through glass windows. Infrared optics are more expensive than glass lenses for this reason.

The performance-price trade-off favors uncooled imagers for targets at distances of 1 km or less, and cooled imagers for targets at distances greater than 2 km. For targets between 1 and 2 km, the selection will be governed by operational factors, such as reliability and maintainability, and by equipment cost.

Thermal imagers can be used in most cases with video analytics, and particularly with video motion detection analytics, because their white-on-black background target images often provide sufficient contrast for the analytical functions to perform acceptably. Analytic performance can also be enhanced by reversing the image polarization (i.e., show targets as black on a white background).

As in the case of video sensors, FLIR performance under actual operating conditions should be validated before FLIRs are specified as sensors. Infrared imager performance should be determined during the ConOps, and then set forth in equipment design specifications. The parameters to be specified should include:

- System responsivity : Usually in the form of an S-shaped curve and defines the range of performance

- Noise equivalent temperature difference: Measures the infrared detector sensitivity and should be less than 100mK
- Dynamic range: Describes the ability of an infrared detector to produce an image over a wide variety of infrared emissions
- Wavelength sensitivity: Distinguishes between various wavelengths in the infrared spectrum
- Array size: Varies by type of thermal camera (cooled vs uncooled) and determines image resolution
- Detector pitch: Pixel spacing should be 60 microns or less to achieve adequate sensitivity and resolution

Countermeasures have also been developed for thermal imagers. These measures include coatings and materials developed to absorb infrared energy and/or reduce the self-emissivity of an object, whether it is a vehicle or a person. This makes it even more important to secure a perimeter with multiple technologies so that an intruder cannot “game’ the security system.

Operationally, it is important to understand the relationship between infrared wavelength and imager resolution. Imager resolution is proportional to the inverse of wavelength. For imagers having the same lens focal length, the resolution (detail) of an MWIR image will typically appear on a monitor to be about one-third that of a CCTV camera or NIR image-intensified array, and an LWIR imager will appear to have about one-tenth of the resolving power of a CCTV image.

During system design, attention should be given to the selection of cooled or uncooled arrays, which will impact both performance and cost. Cryogenic cooling can provide higher resolutions at longer ranges than uncooled arrays, but these systems are costlier and reliability is dependent on the cryogenic cooler. Uncooled arrays can extend ranges by using large apertures, but these systems use costlier lenses. The range-performance-cost trades are generally for targets at 1.5 to 2.5 km, with uncooled sensors being better for targets within 1.5 to 2 km and cooled arrays better for sensing targets at longer ranges. In some situations, multiple uncooled sensors can be configured for area coverage equivalent to cooled sensors.

It is also important to consider how imager performance is affected by environmental factors. Thermal imagers sense temperature *differential*; if a body is at the same temperature as the environment, it may not be “seen” by the imager or the detection distance may be greatly reduced; this is a situation to be addressed in specifying thermal imagers for warm climate operations. For operations in rainy and snowy conditions, the clothing of persons in the scene may absorb sufficient amounts of moisture to effectively mask their body temperatures, which reduces detection ranges. For operations in fog, the density of fog will affect detection performance and will vary with the band of operation. Similarly, in the presence of smoke, the chemical composition and density of the smoke will affect detection performance.

12.6 Intelligent Video

Intelligent video refers to enhancements of a camera’s output images. Intelligent video originated with motion detection, for which a designated area of interest is drawn electronically on a monitor. An operator can then be alerted to an event as it happens, greatly reducing the need for operators to stare at video monitors for long periods of time to notice an anomaly.

The effectiveness of this technology has improved greatly. Systems now are able to compensate for the sun progressing across its arc during the day, and for environmental effects such as blowing trees, which created false positive alerts in early systems. Intelligent systems can also detect multiple objects in a scene; exclude designated areas of a scene; track objects as they move across the scene; generate position coordinates and speed data for these objects as they move; and in some cases, distinguish types of targets by class, e.g., distinguishing between humans, animals, and vehicles. The value of these functions depends on the user's operational requirements (preferably determined in the ConOps) and, especially, their probability of detection and false alarm rate.

Intelligent video functions apply mainly to fixed cameras, but, under certain conditions, object detection and tracking can span multiple cameras, even as these cameras are panned and tilted, stitching together a continuing tracking image.

Intelligent video is also able to analyze an object and determine whether it is a possible concern, based on behavioral "rules" established by a security administrator. A basic application of this is monitoring of passenger traffic in a loading bridge. If persons exiting an aircraft reverse their course, a camera monitoring that loading bridge will see the change in direction and use tracking software to notify the SOC. Intelligent video can also associate behavior or events, including events detected by other sensors, such as thermal imaging cameras and ground surveillance radars, to further aid security operations.

The key to "fusing" these sensor inputs is showing them on monitors, or a video wall associated with one or more live images and layout diagrams, including maps and engineering drawings that can be animated. A more advanced "fusion" process shows the airport in graphic form starting from a point above the airport and electronically zooming down to a specific point based on alerts from access control devices or radio frequency tags (RFID). Using this technology, persons or devices that have RFID tags, including baggage, can be tracked across an airport using wireless networks and be located precisely at all times.

All of these features and advanced capabilities come at a price. During development of the ConOps, airports must carefully weigh the benefits and costs, especially with regard to how these features contribute to established operational requirements, how they are to be implemented, and their downstream support requirements, including the complexity of operator training.

Intelligent video capabilities, which are implemented entirely in software, may have a cost advantage, depending on software licensing rates, but may also impact hardware by requiring more powerful servers and increased hard drive capacity, or a reduction in the number of video cameras that a server can support simultaneously.

A program implemented as a new hardware appliance may impact available equipment space, electrical power, and network interfacing, in addition to requiring software compatibility and maintenance of the new equipment.

These types of issues should be considered in evaluating new system features and capabilities. Still, as noted early in this section, airport security should be more concerned with the potential operational value added than technical details such as software algorithms. In the case of object detection and tracking, for example, it might be operationally useful to express the evaluation process as:

- Detect and track at least two attempted intrusions of multiple perimeter fence segments simultaneously
- Maintain tracks and generate horizontal position coordinates for intruders as they move inside the airport property

- Superimpose the intruder tracks on maps and/or drawings of the airport and its facilities at monitors in the SOC
- Demonstrate 3D visualization of the events, in real time, on the operator monitors
- Provide the SOC with recommended actions, such as LEO alerts

12.6.1 Video Analytics

Video analytics are a form of intelligent video in which decision rules, implemented in software, apply specific behaviors and/or changes derived from the video signal.

When properly configured, video analytics can greatly enhance video surveillance capabilities and reduce the workload of monitoring personnel, but they should be carefully planned and installed, with appropriate training. Video analytics performance is sensitive to viewing conditions including lighting, weather, camera angle, distance to a target, other activity in the camera field of view, and changes in the viewing background. Users should assume that proposed video analytics have been designed to function with full video signals (100 IREs and 50 dB signal to noise ratio or greater) unless the manufacturer is able to provide data on performance under less than optimal lighting and environmental conditions.

False alarm rate is the driver for user acceptance of video analytics. Even in a relatively small network of 100 cameras, one false alarm per camera per day will often cause a user to turn off the analytics. It should be documented how the analytics are to perform, how they are to be tested to verify performance across the range of the user’s conditions, and how they will benefit the user. In some cases, operational performance can only be determined by testing across the range of local operational conditions found at the airport, but not in the laboratory.

There is no substitute for testing candidate cameras and candidate analytics in the user’s environment, preferably over a period of at least several days and different conditions, during or prior to schematic design. The testing should validate camera compatibility and the extent to which the analytics can be “tuned” to achieve an acceptable false alarm rate *to the user*.

The type of artificial lighting can affect analytics performance. For example, sodium vapor lamps commonly used for street lighting have a very narrow spectral distribution centered at 590 nm. There is very little area under the spectrum curve, which limits the energy that a camera can detect. Changing from sodium vapor lamps to modern LED) lamps, which have a broad color distribution, can be the difference between usable and unusable video analytics under nighttime conditions. The analytics should be able to learn and apply environmental variables, and suppress false alerts without sacrificing performance. Reducing sensitivity to minimize false alarms is not a viable solution if it also reduces performance below what is needed.

Video analytics can be associated with both color and monochrome video cameras, as well as with thermal cameras. Typical applications are:

- Associated with fixed cameras
  - People congestion
  - People counting
  - Abandoned object detection.
  - Human tailgating

  - Basic detection, i.e., monitoring a portal
  - Parked vehicle detection
  - Advanced motion detection for determining the direction of vehicle and human intruders
- Associated with PTZ cameras
  - PTZ scan and dwell modeled for vehicle and human intrusion
  - Hand-off of fixed to PTZ for target tracking, e.g., handing off an image from a fixed camera to follow a moving target, perhaps by a series of cameras

Each of the analytics functions selected by a user should be specified, including how the function will be assessed and validated during acceptance testing.

There are two general ways in which video analytics may be configured:

- Server-based analytics, in which the software runs on servers in the data center or SOC
- Camera-based analytics, in which the software is embedded in cameras at the edge of the IT network, in some instances with video storage also being embedded in the cameras

There are pros and cons to both approaches, with potentially significant operational and maintenance cost implications. During schematic design, both approaches should be evaluated against the user's operational requirements and the architecture and capabilities of the IT network that is to support the video cameras.

Server-based analytics leverage the computing power of modern IT servers, storage devices, and maintenance availability in the IT datacenter. Server-based analytics enable a user to select best-of-class analytical software independent of camera capabilities; it is unlikely that any one manufacturer will have best-in-class software as well as the cameras best suited for specific applications. At the same time, a server may support several cameras, so loss of the server will mean the loss of multiple cameras. This also applies to centralized video storage devices. There are ways to mitigate such problems, but they introduce their own complexities and costs.

Server-based analytics buffer the user from a closed, proprietary, single-source video solution, which may have limited upgrade potential, and would be expensive to replace if problems develop with either the analytics or the cameras (or if the manufacturer goes out of business).

Camera-based analytics leverage compression at the source, reducing the bandwidth required for video transmission over an IT network. Storage may also be embedded in the camera. Systems can incorporate solid-state storage chips for short term storage. Hard drives can be used for longer term storage, running only for short periods of time, extending their life, and improving their reliability (a major issue with video hard drives, which typically run 90 percent or more of the time in "write" mode). For outdoor cameras, all embedded elements must meet local environmental requirements and, in a desert or tropical area, this may require supplemental cooling. Being able to service remotely located cameras, some of which may to be mounted atop poles, is an issue when the camera contains the "smart" components of a video network.

The advantages claimed for embedded analytics, with or without embedded storage, can also be realized by performing the analytic functions in an appliance installed at or near a camera, with or without local storage. Such an appliance could support one or more cameras, depending on where the cameras are installed and their accessibility to a network node. Use of an external appliance for compression, analytics, storage, and network security (firewall) will enable any type of camera and any compatible analytics software to be selected, thereby eliminating the user's dependence on a single-source supplier.

Having access to multiple suppliers can be a considerable benefit for an airport, especially when complex and evolving technology is involved.

12.7 Video Encoding and Compression

How a video stream is compressed and stored in digital format depends on (a) the type of video camera, (b) the storage architecture, and (c) the available network transmission bandwidth if the video is transmitted over an IT network.

More than 90 percent of the CCTV cameras installed worldwide are analog cameras. The percentage is even higher for thermal (infrared) cameras. In the case of CCTV cameras, the percentage will decrease as more IP cameras are installed, but in the near term, analog cameras dominate the installed base. Encoders will still be needed to digitize and compress streaming video for transmission over digital networks and to integrate with video storage devices. Encoders will also provide the interface between analog cameras and DVRs, and the interface with VMS that do not support DVRs.

Realizing the benefits of video compression protocols, and avoiding problems or image degradation requires consideration of scene complexity, streaming mode, video frame rate, the way compression protocol is configured and applied (constant and variable bit rates and levels of quantification), and other parameters.

Several video compression protocols are available. The most commonly used are MPEG, MJPEG-4, and H.264 (also known as MJPEG-4 AVC) compression protocols.

The H.264 protocol has become the compression standard of choice for surveillance video because, under most conditions, it provides better compression with comparable image quality compared to MPEG-4 when images are viewed on a monitor. The compression advantage of H.264 may be important if network transmission bandwidth is an issue. H.264 can also reduce hard drive storage requirements, although even terabyte capacity hard drives are now relatively inexpensive.

The H.264 protocol is available in several types, and the ratio of full frames to incremental frames can be varied, affecting CPU requirements as well as viewing quality. H.264 quality is sensitive to frame rate; at 7.5 fps, the small number of full frames may affect viewing quality as well as the functioning of video analytics under less than ideal conditions. For scenes with high levels of activity, similar problems may arise at 7.5 fps. For these reasons, setup should be carefully addressed and, if any doubts arise, the proposed configuration be subjected to testing with the intended cameras and encoders to ensure that the specified output quality will be realized.

The H.265 is a relatively new standard, having been approved in January 2013. Also known as the High Efficiency Video Coding, H.265 is touted as reducing streaming video bit rates by 25 to 50 percent compared to H.264, which is an advantage for video storage requirements. To achieve this improved performance, camera chipsets must be upgraded and additional server resources may be required for the higher computational demands of H.265. Bandwidth may also be an issue, as H.265 bit rates may spike above H.264 levels at night in the presence of headlights and other point light sources.

Some camera manufacturers are developing enhancements to H.264 for these reasons. Known as “smart codecs” or “H.264+”, the objective is to extend H.264 compression to levels comparable to H.265, thereby avoiding H.265 issues and costs. These solutions are proprietary to each camera manufacturer.

Evaluating compression alternatives should be addressed during the ConOps as an element of video transmission storage requirements, with the most promising solutions then validated during Basis-of-Design trade studies. If an airport is running extensive video analytics on the same servers as video compression software, tests should be performed to ensure that the video analytic functions will be properly supported. If IP cameras are used, the digital conversion and compression will normally be done at the cameras, with the output formatted for transmission over a local area network. In this case, the bandwidth and processing capabilities of the camera electronics will determine the maximum resolution and frame rate that can be displayed and recorded. Unlike analog video cameras, it is common practice for IP cameras to be specified with several resolution-frame rate combinations that reflect the limitations of the embedded electronics; for example, cameras could have 4CIF resolution at 7 fps or CIF resolution at 30 fps, but not 4CIF at 30 fps. It is important for the airport user to understand these specifications and to relate them to the operational performance requirements.

12.8 Video Management Systems

In enterprise-type security systems, video cameras almost always distribute video to viewing stations and storage media through a VMS. A VMS manages video images received from multiple cameras across a network. It then enables the user to operate on the video streams, distribute the video, store the video, and perform other functions.

A VMS may store video in several ways. DVRs, which serve analog cameras, or on Network Video Recorders (NVR), which serve IP cameras (hybrid DVRs have been introduced that support both IP and analog cameras), are commonly used, but it is also possible to directly write to network storage systems (see the discussion of Network Attached Storage and Storage Area Network under Section 13.2.13).

A VMS that includes DVRs and NVRs may lock the user into a proprietary solution, i.e., limiting the choice of cameras, video analytics, and other video elements to those available from the DVR or NVR manufacturer.

A software-based VMS solution is an application package designed to support many video hardware packages, and is designed to support many camera, DVR, and NVR manufacturers. These applications typically provide a long list of functions, which is both good and bad—good because it gives an operator a wide range of capabilities, and bad because the demands on the operator, and the associated training required, increase with complexity.

A rule-of-thumb for VMS systems is that 80 percent of the operators use 20 percent or less of the advertised features. Having a long list of available functions does not mean that all of them will be used, or that all of them are needed. The key is to identify during schematic design what functions are really required, and then select a VMS that provides them in the most user-friendly manner, with the least complexity and preferably using open standards.

VMS architectures differ widely, as does support for third-party cameras and video analytics. Indeed, some VMS packages only support the manufacturer's own cameras and analytics, which would prevent a user from specifying third-party products and poses sole-source procurement and support risks. Applying ONVIF and/or PSIA industry standards provides a basis for establishing general hardware and software compatibility and interoperability. If a user intends to specify cameras and video analytics independently of the VMS, the VMS provider, which for enterprise systems may be a system integrator, should be required to guarantee interoperability of all video elements (hardware and software) and back this up with a demonstration, which also includes setup procedures, matching features to user requirements, and ease of use.

Some of the other issues to be considered and evaluated when assessing VMS suitability and how well a particular VMS meets the user's requirements for a video surveillance system include:

- Architecture: Most VMS systems use a client-server architecture. If the central servers fail, so does the entire system, unless the manufacturer includes failover measures and redundancy. The alternative is to use a peer-to-peer architecture, but this requires that the distributed databases be properly synchronized. Users should evaluate these measures and how they are applied.
- Basic Functions: A VMS provider should demonstrate how cameras are called up, how images are monitored and processed, how images are stored and recalled, and how third-party applications are integrated into the operator screens. In some VMS, many functions can be accessed with a few clicks of a mouse, while in others, the operator may have to click through several layers of menus on the screen. Menu-driven applications may afford greater flexibility, but where extensive menu trees are involved, more capable operators and more intensive operator training may be necessary, and lower-menu activity may be missed altogether. Accessing third-party applications, such as video analytics, may differ from the VMS methodology, and may require entirely different setup procedures. The user should become familiar with all of these functions and the operator menus to access them during the assessment process.
- Feature Set Customization: The software should enable a user to lockout all but the most needed features, and do to this for each operator station.
- Scene Viewing: Some VMS systems offer scene stitching, which allows an operator to stitch or merge the imagery from multiple adjacent cameras, and can greatly assist in coping with areas of high activity. The user should decide if this feature is important.
- Physical Access Control System and Intrusion Detection System Integration: All VMS systems offer some level of integration for alarms and events, but the extent of integration and how the data are presented, e.g., with or without geo-referencing overlaid on photographs and/or CAD drawings of the facility, should be demonstrated to the user's satisfaction.
- VMS Throughout: For large systems, VMS performance on managing heavy loads and stresses on the system should be evaluated. The VMS should enable a user to apply rules for prioritizing different types and locations of traffic under these conditions.
- Investigations and Case Management: Most VMS systems provide only basic search and investigative functionality. The user should decide if search and case management capabilities are important.
- Monitoring and Auditing: All VMS systems log activity data, and provide for recall and analysis of the event data, but the implementations vary widely. User requirements for these functions also differ, which complicates the evaluation process. VMS pricing also varies widely, ranging from single-server licenses to multi-tiered license structures for different levels of functionality. No price-per-function metric is available to assist a user in making a value assessment, i.e., comparing functional capabilities to their associated prices.

12.9 Video Storage

Video storage, whether in analog (tape) or digital (hard drive, optical media, or tape) formats, can present significant design, management, and cost challenges, especially for airports having several hundred or more video cameras.

During the ConOps, the first step is to determine the video that must be stored, the period of time it must be kept, and the quality level required. These are operational not technical requirements, and they include assessing the frequency and consequences of potential threats. At this time, there are no approved standards or TSA regulations that govern how an airport operator is to define and apply them.

Video may also be stored in the cameras themselves or in directly connected Edge appliances to reduce network bandwidth requirements, but this is temporary storage and not “record” or archival storage.

The network video streams may include all frames, even those tagged as motion frames or video analytic frames. The user can choose to store all video frames in several ways depending on the requirements defined in the ConOps. For example, all video, including motion video, could be stored for one or more days so that if an event occurs, what took place before and after the event will be available for examination. Or, all video frames could be stored for one or a few days, with only tagged frames stored for a longer period of time. There are many possible scenarios that can be considered.

Many airport operators have elected to store video for 30 days, but this is not a standard. Other airports store video only for 7 days while, in extreme cases, a year or more may be driven by policy concerns, including public safety and risk management.

Typically, motion or video analytics frames represent 15 to 20 percent of all frames— much of which is normal activity and not necessarily of any concern; the other frames represent no action and routine surveillance.

Storing only tagged frames for all cameras after a few days can significantly reduce video storage costs, equipment rack space, and electrical power, including UPS backup, HVAC cooling, and system management. Unless there is a compelling reason to store all frames for more than a few days, storing only tagged frames after a time determined during the ConOps will better serve the airport’s interests.

Digital video streams can be transmitted at full video frame-rate, which in the United States is 60 fps at a reduced frame rate as low as 1 fps. If video analytics are used, the frame rate should be at least 7.5 fps with 15 fps used for areas of high activity. The video analytics vendor should confirm this and demonstrate that it works properly.

Depending on the VMS capabilities, it may be possible to also capture tagged frames at a reduced frame rate after several days, further reducing storage equipment acquisition and support costs. These are measures to be examined during schematic design.

Internal storage, using DVRs and NVRs, lacks the capacity to support the outputs of hundreds of cameras over a typical 30-day scenario. Attached storage, using external hard drives, is likely to be needed for large video surveillance systems. The two most common types are Network Attached Storage and Storage Area Network that are arranged in modular clusters scaled for the required amount of storage, that employ Redundant Array of Independent Disks (RAID) for protection against hard drive or power failure, and that are networked over the local area network. Additional information on RAID storage configurations is contained in Section 13 regarding Communications and IT.

The configuration, capacity, networking, and equipment required for video storage are properly determined during schematic design. For large video systems, storage clusters should be less expensive than cascading DVR and NVR units, be easier to manage, provide higher levels of reliability using hot-swappable components and reconfigurable-on-the-fly volumes, and be more compatible with the use of MP cameras.

Streaming video is a write-intensive storage process; standard hard drives were never designed for this type of continuous operation. Some hard drive manufacturers offer so-called audio-video class hard drives for video storage, which claim higher reliability and provide longer operating warranty periods at nominal increases in cost. Planners should consider such products during schematic design.

The system may also include off-site storage for protection against catastrophic events at the airport, such as floods or fire, the need for which should be determined during the ConOps.

For airport video to serve the needs of law enforcement, the means of storage and access to the stored imagery will require special attention once image quality requirements have been resolved. If the video imagery is stored digitally, issues of secure storage and information authentication will arise, and will require that the airport establish consistent, valid, and verifiable procedures for controlling access to and authenticating the digitally stored imagery. A digitally stored image can be easily edited to the point that even forensic experts cannot agree whether an image has been manipulated. Access to servers and digital storage volumes may require special physical storage and access control provisions, such as biometric identification of authorized personnel.

Video image transfers across the airport network or over the internet present special problems, which should be addressed by both airport security and the airport IT department. If file encryption is to be used, an encryption technique such as the U.S. government-approved Advanced Encryption Standard should be considered.

12.10 System Design and Infrastructure

Typically, video surveillance systems have been designed as components of a broader facility security system, or sometimes as stand-alone systems. However, this is changing as IT networks become more capable and video security systems become smarter, enabling multiple users in the security community to monitor an event in real time from different locations over the internet or wireless networks.

The result is that video surveillance systems are increasingly being integrated with an airport's IT network, with video camera outputs traveling over the IT infrastructure rather than a dedicated security infrastructure. This trend toward networked video surveillance will grow as the underlying digital technology continues to improve.

In a typical IT network, video camera outputs are digitized and compressed at the camera heads, or are transmitted using fiber optic converters to a network device that digitizes and compresses the signals. The digital data streams can then be transmitted over the network infrastructure, assuming adequate transmission bandwidth exists for the number of cameras involved.

System planning should also address the following system and operational issues:

- Privacy Protection: Security system design should provide for the control of internal permissions and authorizations for access to, copying of, and disseminating data. Supervisory and audit controls should be designed to mitigate the possibility of data misuse.
- Records Retention: Planners and designers should address retention requirements established by the ConOps, including possible Freedom of Information Act, forensic, legal, and insurance requirements.
- SSI Regulation: Schematic design should address the extent to which video imagery is available under TSA SSI regulations, and ensure that SSI data is properly identified and safeguarded,

including permissions and authorizations with respect to access, use, and dissemination of video data.

- Video Quality: Airport security normally does not require identification-quality video imagery, in contrast to law enforcement, which focuses on identifying persons. As the standard criteria indicate, identification-quality video requires several times more information than detection, orientation, or recognition video, which translates into more capable and costlier video surveillance cameras, lenses, and storage devices. During development of the ConOps, specific locations where identification-quality video imagery *may* be required should be identified and tagged for schematic design. It may also be necessary to establish a chain of custody of video data that is going to be utilized as evidence to ensure the integrity of that data.

12.10.1 System Integration and PSIMs

PSIM is a command and control center concept intended to improve situational awareness, situation management, and situation reconstruction.

- *Situational awareness* is about an operator being fully aware of events and activities and their ongoing status. Situation management is about an operator knowing what to do next, or in case a task may be automated, ensuring that the system knows what to do next, without delay and with complete consistency.
- *Situation management* is particularly important for scenarios where operators are experiencing heavy incident workloads, or during periods of highly stressful incidents, such as multiple simultaneous events, when operators are fairly new and inexperienced, or when there are changes to the SOPs that require added training classes.
- *Situation reconstruction* builds on lessons from experience. PSIM solutions typically provide rich reports because they automatically combine data from multiple systems (e.g. video, access, fire, etc.), and permits an event to be reconstructed to see how it unfolded. Virtual re-enactment of an incident provides insight as to how people, systems, and processes performed, and what changes should be made to improve system effectiveness.

PSIM software is advertised as the portal for all other components of an airport security system, consolidating and prioritizing relevant information from these components, and presenting the most likely functions (e.g., open a door, move a camera, or acknowledge a smoke alarm) for response actions. For situation management, and using preset digital representations of standard operating procedures, a PSIM is supposed to lead operators through the process of who should do what and when.

PSIM and VMS software overlap to some extent; for many airports there is very little difference between these approaches. Many VMS software programs do a satisfactory job of integrating other systems, although the range of systems to be supported may be limited. With a PSIM, subsystem agnostic capabilities are built in for a wide range of applications; over time, this results in many elements of integration becoming available as off-the-shelf modules.

A potential single point of failure is an upgrade to the PSIM itself, which could affect all the subsystem connections. For this reason, good PSIM software will isolate core application functionality from the gateways or connections to the components, and coding is designed to allow PSIM upgrading without affecting the integrated components.

The PSIM should accept new components to be integrated without changing the version of the software. This independence is critical; if adding one new component changes the core software, this could, at best, require complete system testing from scratch, and, at worst, require that all the other component integrations be updated. Each component might eventually require expansion (e.g. more cameras, more doors or more perimeter sensors), and a PSIM should be designed to cope with such expansions. It is rare to see limits on sensor counts, but there is still a practical limit unique to each PSIM, its server, the database and physical storage it uses, each combination of components and sensors, and each IT network and available bandwidth. As the system expands, there may or may not be performance implications.

Because it uses a hierarchical architecture, PSIM software can provide for reconstructing an incident for training, event evidence, or continuous system improvement. For example, it is easier to understand how an entire situation started and evolved if there is a way to present the video, the audio (including radios), the status of all the relevant sensors, and visually tracking mobile assets on a GIS map. An integrated and interactive report is complementary to a static audit report of who did what and when, but is arguably more valuable because of the ability to re-enact the incident in real time.

12.11 Lighting

Whether lighting is exterior or interior, the placement and amount of lighting 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. Terminals with large glass facades, for example, 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, visible street lighting can be used to raise the illumination in such areas to a level compatible with camera sensitivity.

Near-infrared illuminators, which cannot be seen by the naked eye but can be sensed by a CCD/CMOS array, can also 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 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.

At this time, there are no U.S. 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 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. For exterior lighting, metal halide lamps generally provide better illumination than sodium or fluorescent lamps, and better match the spectrum sensitivity of video cameras; however, metal halide lamps are also more costly.

Another option, which is now commercialized, is the use of LEDs. LED lamps are now widely used for highway lighting and for illuminating critical infrastructure assets on government facilities. These solid-state devices are smaller and use much less power than conventional lamps for equivalent outputs. Their broad spectra also match the sensitivity of CCD cameras better than the spectra of sodium vapor lamps.

The lighting industry has set a goal for white LEDs output of 150 lumens per watt. For airports, replacing sodium vapor lamps along perimeters with more efficient LED lighting can enable video cameras to function with video analytics at night, thereby avoiding the cost of installing power-intensive infrared illuminators, expensive intensified cameras, or thermal (infrared) imaging cameras.

LED lamp fixtures are available in units that can replace sodium vapor lamp fixtures in the field without having to upgrade the local electrical infrastructure.

It is advisable for airport personnel to evaluate lighting in areas to be 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.

12.12 Trends

- Greater use of the ConOps process to establish operational requirements for video surveillance performance (the four performance levels: detection, classification, recognition, and identification)
- Greater use of ceiling and wall-mounted MP cameras, some containing multiple camera heads, for area coverage to reduce camera count and network cabling
- Continued reduction in the cost of uncooled infrared/thermal cameras and detector pixel size, to supplement visual cameras
- Increased use of LED illuminators in visual cameras to improve imaging resolution in areas of poor illumination
- Greater use of wireless networks to connect airport security personnel on the move with events being managed in the SOC
- Greater use of dedicated networks for physical security systems, driven by bandwidth requirements for MP cameras and large camera counts
- Storage of routine, non-event video streams in the cloud to focus local resources on event-related activities
- Wireless distribution of video streams, especially to smartphone users and to offsite control centers
- Encryption of critical video using multi-factor biometrics to prevent unauthorized access
- Increasing SOC integration, to include superimposing various imagery onto map or CADD-based backgrounds to improve overall situational awareness
- Increased use of facial recognition, iris identification, and other biometrics (see Section 10)

12.13 Checklist

Video Surveillance Checklist

- □ Develop ConOps requirements
  - Survey stakeholders
  - Involve IT department
  - Set space, budget limits
  - Legacy systems – retain or replace
  - Public/media access
  - ID social media usage
  - Interoperability requirements
- □ Video Surveillance Planning and Design
  - Determine standards
  - Set video objectives (lighting, weather, range, resolution, surveillance areas, configuration)
  - Assess IR illumination
  - Assess video analytics
    - Validate performance (detect, orient, classify, identify)
  - CADD for field-of-view
  - Plan wireless expansion
  - Evaluate cybersecurity
- □ Video Management, Storage and SOC Integration
  - Estimate bandwidth requirements for camera-to-SOC
  - Assess compression software options (H-264 vs H-265Z)
  - Identify necessary video management system software
  - Assess costs of functionality for 3rd party devices
  - Evaluate video storage alternatives – event/non-event
  - Establish requirements for redundancy, backup

Detailed design information for the SOC applications, networking, communications, CCTV, and supplementary functionality can be found in complementary sections throughout this document, as well as in industry and government guidance documents noted in the bibliography.

SECTION 13: COMMUNICATIONS, IT, POWER, & CABLING

13.1 Introduction

Prior to this section, we have been dealing with design guidelines for functional areas of airport security systems. This section focuses on airport communications, especially on networked communications, but also addresses critical supporting infrastructure elements such as power, communications, and cabling infrastructure. These elements are essential to support an airport enterprise architecture that hosts multiple, and potentially integrated, security applications such as CCTV, access control systems, identification management systems, and perimeter intrusion detection systems.

From an enterprise architecture perspective, airport operators since the mid-1990s have been installing high-speed fiber optic networks to support the connectivity and bandwidth required by the variety of operational systems such as building, financial, passenger processing, and security. These networks have been supplemented with wireless capabilities supporting a variety of communications protocols. Additionally, a growing number of airports have been implementing robust converged networks, using resilient architectures to support the data, voice, and video demands throughout the airport.

An airport communication network should be supported by logical data systems architecture based on industry open-system standards to allow a variety of applications and systems to easily integrate onto the network. The airport data systems architecture should also be flexible enough to support a variety of applications and to allow information to be shared among multiple security-related systems at the airport.

Due to the mission-critical nature of security, it is essential that supporting elements such as communications, power, 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 distribution layer, and to minimize single points 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. For large security systems, especially those having hundreds of video cameras, a dedicated network for security applications may be more cost-effective as well as more secure than running security applications over a common airport IT network.

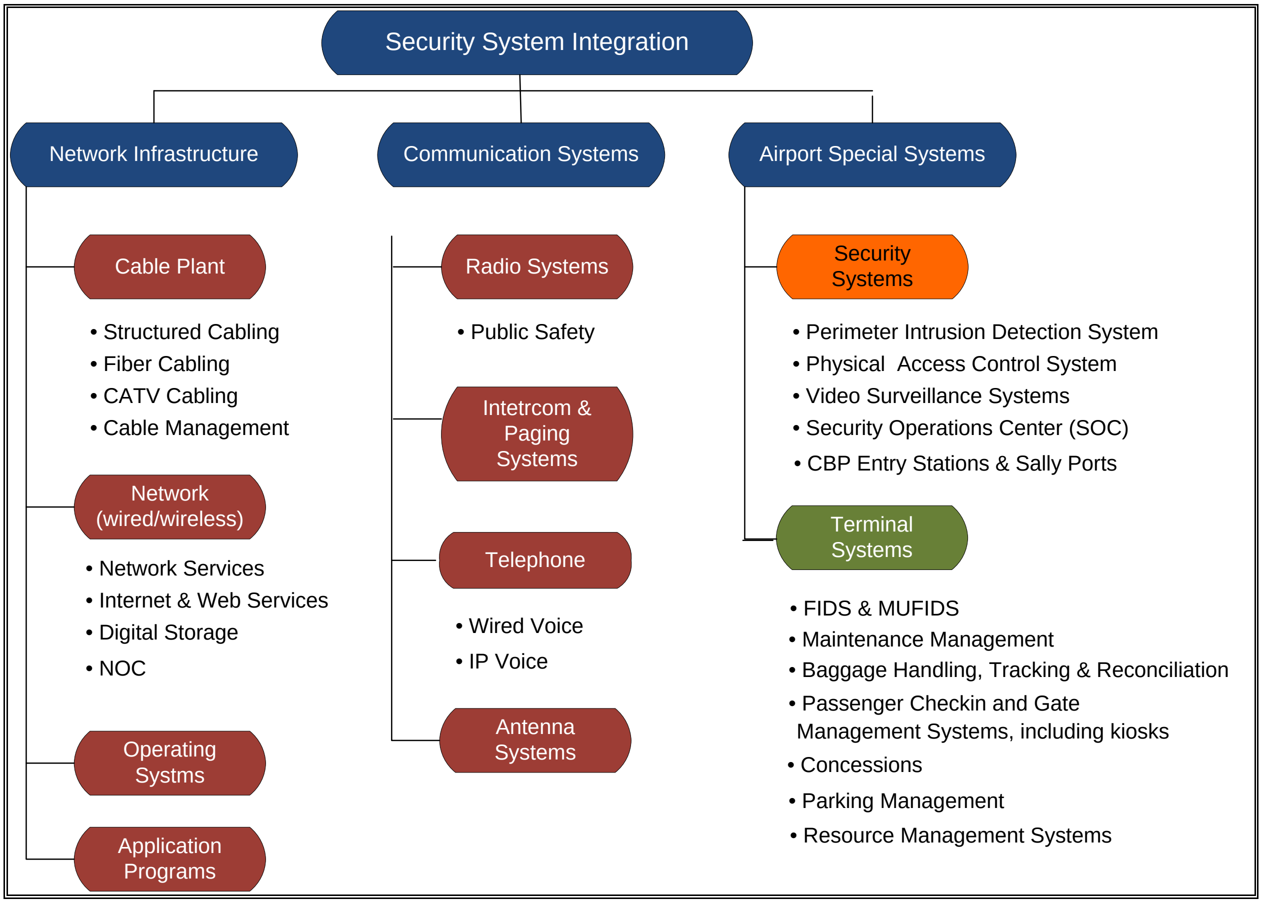
The communications network supporting security systems should not only have high system availability, but also should ensure data integrity and data security. Airport operators should ensure that appropriate network information/data security solutions and protocols are incorporated within its enterprise network architecture, not only at the network level, but also at the application/session level. Loss of functionality or data integrity on these systems risks jeopardizing the airport’s safety and security. While some of the most critical data being transmitted pertains to the airport’s access control and monitoring system, the security of other data and systems, such as flight information, lighting systems, cooling systems, and UHF/VHF radio systems, is vital to airport operations. Unauthorized access to virtually any airport data or system could impact flight operations or threaten public safety.

13.2 Communications and IT Infrastructure

The design process for the IT infrastructure 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. Figure

13-1 illustrates the departmental relationships that may be important to IT networks to ensure adequate functionality for security and related services.

Figure 13-1. Airport Networked Communications

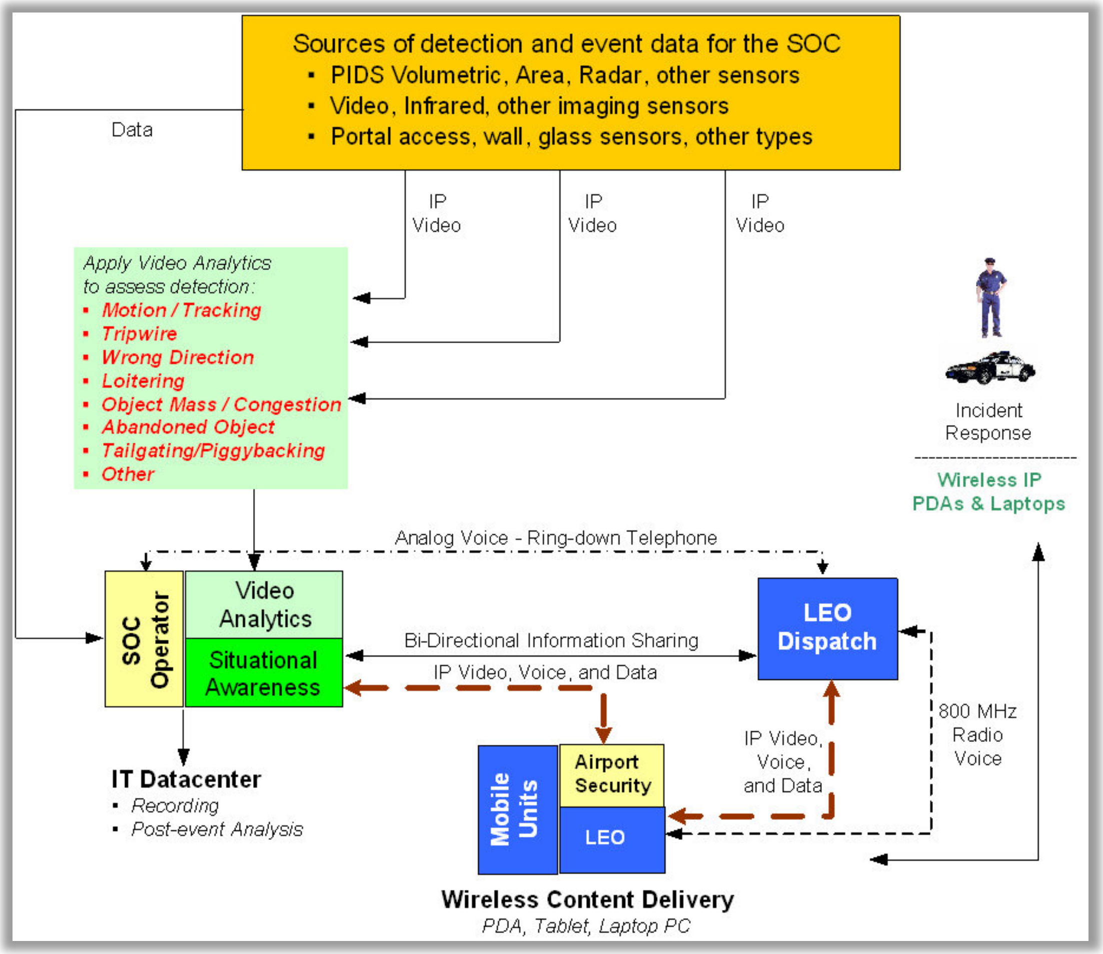


13.2.1 Security Operations Center

A Security Operations Center (SOC) is not simply a monitor of throughput at portals and within Secured Areas. Its parallel purpose is to recognize activity within its domain; process and sort data at the SOC level for indications of intrusions, anomalies, and non-standard conditions; identify trends; and initiate response and resolution of alerts and alarms. Effective resolution of events depends on having full and accurate data, since missing or erroneous data can cause the process and/or the SOC operator to misinterpret the event, resulting in an inappropriate response. See Section 15 for additional information on system integration in the SOC.

For a police-centric or security-centric SOC, Figure 13-2 illustrates the communication flows that may be present and require IT support. The configuration and functionality of the SOC will depend on its role and relationship with responder dispatch and incident management functions.

Figure 13-2. Communication Flows


Sources of detection and event data for the SOC
PIDS Volumetric, Area, Radar, other sensors
Video, Infrared, other imaging sensors
Portal access, wall, glass sensors, other types
Data
IP Video
IP Video
IP Video
Apply Video Analytics to assess detection:
Motion / Tracking
Tripwire
Wrong Direction
Loitering
Object Mass / Congestion
Abandoned Object
Tailgating/Piggybacking
Other
Incident Response
Wireless IP PDAs & Laptops
Analog Voice - Ring-down Telephone
SOC Operator
Video Analytics
Situational Awareness
LEO Dispatch
Bi-Directional Information Sharing
IP Video, Voice, and Data
800 MHz Radio Voice
IP Video, Voice, and Data
IT Datacenter
Recording
Post-event Analysis
Mobile Units
Airport Security
LEO
Wireless Content Delivery
PDA, Tablet, Laptop PC

Source: TranSecure, Inc.

All of these functions may be performed in the SOC, but at many airports, the dispatch and incident management functions are performed in a separate and/or consolidated Police Dispatch Center. Either arrangement is workable with the proper information flow.

13.2.2 Network Design Objectives

It is imperative to set clear design objectives at the outset of the design process by identifying 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 those 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.

13.2.3 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 equipment in the distribution network, and 1 Gigabit (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.

For video transmission, a network using 10GbE or higher data rate equipment can reduce end-to-end streaming delays (latency), resulting in improved video transmission across the network. It may also reduce equipment acquisition and maintenance costs.

- The latency inherent in a three-tier approach should be examined when video is a major network payload.
- The emergence of 10 GbE, and the 40/100 GbE standard approved by the IEEE provides an opportunity to use a two-tier network architecture which, in addition to reducing latency, will result in fewer switches to install, operate, and manage.

13.2.4 Network Standards

Standards are essential for networks to function properly. There are four main networking standards bodies that should be of interest to airports:

- In the United States, the Institute of Electrical and Electronic Engineers (IEEE) publishes standards for networking architectures, such as Ethernet networks; for network devices such as a network switch or a wireless access point; and for a variety of electrical power, communications, and other equipment and systems.
- Also in the United States, the Internet Engineering Task Force (IETF) publishes standards for protocols and devices that operate over the internet.
- In Europe, the main standards bodies are the International Telecommunications Union (ITU) and The International Organization for Standardization (ISO).
- NIST supports these standards bodies, especially in developing best practices for physical network security, e.g., authentication procedures, and for cybersecurity measures.

13.2.5 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. With the exception of wide area network (WAN) connectivity of large data centers, historical evidence for service provider leased lines and data services also points to local area network (LAN) and WAN connection utilization far less than 100 percent.

Oversubscription is inherent in the design of hierarchical networks. There 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 cost 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—where the last traffic into the system is the first traffic dropped—is insufficient for traffic management. 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 airport video surveillance systems are networked, special design consideration must be given to such issues as transmission bandwidth over the network, network headroom allowances, and video storage, including imagery resolution and frame rate, storage duration, and permissions for accessing and viewing stored imagery. Network architecture may involve both centralized and edge-based assets.

Video streaming is a major consumer of bandwidth. Video surveillance applications may include:

- Area surveillance in terminals
- Roadway and curbside baggage
- Cargo loading docks
- Tenant access points
- Baggage handling areas
- Access points to security areas
- Monitoring passenger traffic
- Gate activities
- Monitoring of fenced perimeters
- Vehicle traffic control
- Rental car facilities
- Fuel farm areas
- Parking garage monitoring
- Employee parking areas

13.2.6 Quality of Service

QoS addresses the ability of a network to guarantee different levels of service to selected traffic. Its goal is to prioritize certain traffic flows without making other flows fail, thereby ensuring consistent, guaranteed performance. QoS provisioning is essential for a network carrying SOC voice and 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.

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

13.2.7 Bandwidth Management

Usage of digital technologies for CCTV cameras has increased the typical airport network bandwidth requirements; however, communications network technologies have improved data rate transmission enough to enable airports to design 10 GbE networks. The requirements for frames per second and frame size (video resolution), and video compression techniques will ultimately determine the bandwidth requirements of the security system 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 have to make 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 (CCTV/NVRs, etc.) can be moderate until an alarm or security incident occurs, introducing immediate heavy demands on top of continuing normal loads.

There are some well-proven techniques for reducing the bandwidth loading on a network, such as positioning the NVRs near (in network terms) the camera clusters; use of multicast technology; and use of Activity-Controlled Frame Rate at the camera, whereby the video transmission rate is adjusted based on scene activity.

Given the frequency of moves/adds/changes to airport systems as operations change over time, it is important that all video networking be configured, installed, and tested according to recognized standards and consistent administrative protocols.

The interconnection of these systems is cumulatively referred to as the IT infrastructure, and the supporting cable plant sometimes as the Premises Distribution System (PDS). PDS primarily refers to low voltage cabling, pathway, and network electronics, and does not typically include power elements and enterprise integration platforms. Component portions should be designed and installed to operate seamlessly. The equipment and components of the individual power, communications, and infrastructure systems should be designed, selected, and placed in locations that secure them from tampering and provide for reliable operation during an emergency.

It is unnecessary, and probably impossible, to consider all incident and response scenarios at any airport. Those that are considered should reflect realistic levels of manpower, operator training, and equipment acquisition and support costs. Automated data collection, fusion, analysis, and decision/deployment software may enhance operational capabilities, as long as the software is flexible enough to be tuned to local needs.

The emergence of Ethernet and particularly TCP/IP as industry standards has hastened the migration of mission critical applications away from proprietary networks to shared bandwidth provided by active infrastructures. As a result, the demand for bandwidth and guaranteed QoS continues to increase rapidly, and new applications and hardware are being developed with the assumption of high bandwidth availability. Additionally, future deployments of new hardware-intensive systems and enterprise-wide software applications will increase the need for a well designed and implemented active infrastructure. Components of the active infrastructure are located in telecommunications rooms throughout the airport campus.

13.2.8 Premises Distribution System

The PDS is composed of two elements: the active equipment/software and the passive infrastructure. The passive element includes the fiber optic and metallic conductors that provide physical connectivity throughout the airport.

13.2.8.1 Active Infrastructure

The active element of infrastructure includes all the electronic equipment that transmits, receives, routes, secures, and manages the data that is being transmitted over the passive infrastructure. Several different transport protocols can be employed over the active infrastructure including Ethernet, Token Ring, ATM, Frame Relay, and others. The implemented networking technology determines which data transmission methods can be employed, and the upper limit of the speeds available for transmission.

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 (traditional PBX and Voice over IP), Electronic Visual Information Display Systems, Common Use Passenger Processing Systems, public address systems, building management systems, CCTV, and access control and alarm monitoring systems. 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.

13.2.8.2 Passive Infrastructure

Passive infrastructure systems are composed of the physical cabling components, routing infrastructure (i.e., conduit and cable tray), patch panels, splicing equipment, and termination hardware used for the interconnectivity of communications systems throughout the premises.

Planning and design of the cabling infrastructure for security, communications, and other airport 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 airport communications and security systems are critical to airport operations, reduced multi-year repair times alone warrant careful consideration of these issues.

If security and data transmission media (fiber optic or copper cable) 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 cable separation of the security and data network 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.

Security measures should be taken to protect cabling. Cables, connections, and equipment should be protected from accidental damage, sabotage, and physical wire-tapping. This is usually accomplished by placing security related cabling in Secured Areas; when cabling must pass through public areas, cabling should be protected by metal conduit or electrical-mechanical tubing, and this should extend to telecommunications rooms, where security-related cabling terminates.

Passive infrastructure should be designed in accordance with the most recently published communications industry codes and standards, including BICSI Telecommunications Distribution Methods Manual (TDMM), ANSI/TIA/EIA—568B series, IEEE standards for wired and wireless communications, National Electrical Code (NEC), and local building codes.

The design flexibility of cable trays within a facility should also be reviewed as it provides the most cost-effective and high-density pathway for security and data cabling. As requirements and technologies change, flexibility is a key point to consider, just as excess capacity must be considered for future expansion.

A carefully designed and installed signal ground system is critically important to successful operation of digital data equipment.

Since CCTV became a fixture at airports, video cameras have often been wired directly to an SOC over dedicated copper cable, usually coax type, or over fiber optic cable. The selection of cabling should be based on the transmission distances (longer distances favor fiber), security (fiber cables are difficult to tap and are not susceptible to electromagnetic interference), and cost (fiber has been more expensive than copper cabling, but the gap is closing and the bandwidth advantages of fiber are compelling).

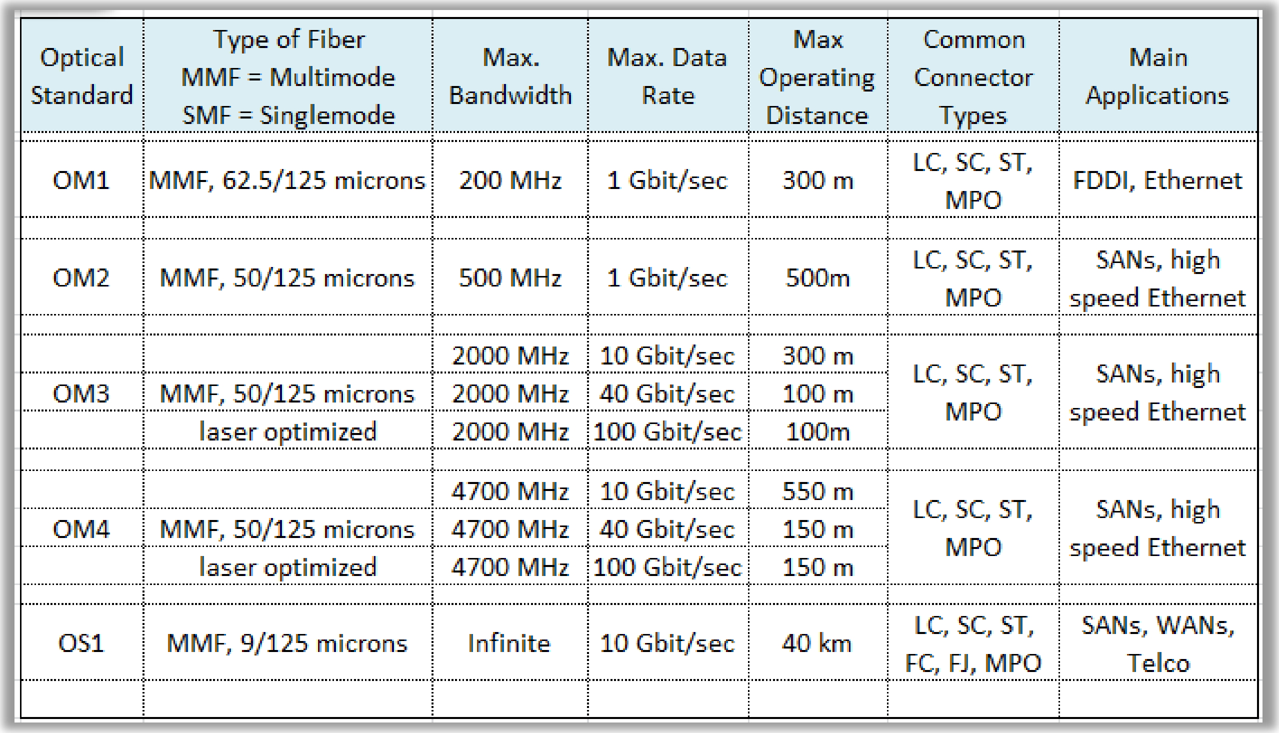
The video cables are then terminated in multiplexers or in matrix switches, from which the signals are routed in analog form to monitors and storage devices such as tape recorders, DVRs, and network storage media.

The cabling model for networked video is quite different. Network requirements rather than video requirements will govern the configuration, and will generally favor connecting cameras as close to the edge of the network as possible rather than connecting the cameras to a central point, especially when more than 100 CCTV cameras are to be networked. When large numbers of cameras are to be networked, having a dedicated network rather than attempting to transmit video over a shared IT infrastructure should be considered.

13.2.8.3 Fiber Optic Backbone

Most airports will network devices using a combination of fiber optic cabling and copper cabling. The choice of cable type depends on requirements for bandwidth and cable distances, potential radio frequency interference, and accessibility, reliability, and life cycle costs. Because of its high bandwidth and relatively long transmission distances, fiber is the preferred mode for interconnecting central network devices, such as servers, as well as edge devices, including cameras around perimeters. Network fiber cabling can be multimode or single-mode types. Transmission distances permitted over network cabling vary by type of cable. The applicable IEEE performance standards for GbE networks are listed in Table 13-1. In 2010, the IEEE approved 40/100 GbE transmissions, which will provide airports with even greater opportunities for networking surveillance video.

Table 13-1. IEEE Fiber Cable Standards and Operating Distances



Optical Standard	Type of Fiber MMF = Multimode SMF = Singlemode	Max. Bandwidth	Max. Data Rate	Max Operating Distance	Common Connector Types	Main Applications
OM1	MMF, 62.5/125 microns	200 MHz	1 Gbit/sec	300 m	LC, SC, ST, MPO	FDDI, Ethernet
OM2	MMF, 50/125 microns	500 MHz	1 Gbit/sec	500m	LC, SC, ST, MPO	SANs, high speed Ethernet
		2000 MHz	10 Gbit/sec	300 m	LC, SC, ST, MPO	SANs, high speed Ethernet
OM3	MMF, 50/125 microns	2000 MHz	40 Gbit/sec	100 m		
	laser optimized	2000 MHz	100 Gbit/sec	100m		
		4700 MHz	10 Gbit/sec	550 m	LC, SC, ST, MPO	SANs, high speed Ethernet
OM4	MMF, 50/125 microns	4700 MHz	40 Gbit/sec	150 m		
	laser optimized	4700 MHz	100 Gbit/sec	150 m		
OS1	MMF, 9/125 microns	Infinite	10 Gbit/sec	40 km	LC, SC, ST, FC, FJ, MPO	SANs, WANs, Telco

Source: TranSecure, Inc.

13.2.8.4 Structured Cabling

Copper cabling is commonly used to connect networked devices to the PDS. This cable plant is known as structured cabling. In the United States, its standards are established by the Telecommunications Industry Association (TIA). These standards define methods of connecting all types of vendors' voice, video, and data equipment over a cabling system that uses a common medium, connectors, and topology.

TIA publishes a set of structured cabling telecommunications standards, which also carry ANSI standard identifiers. These standards are grouped by application as follows:

Common Standards that apply to all users:

- TIA 568-C.0, a generic standard for customer premises
- TIA 569-C for pathways and spaces
- TIA 606-B, an administrative standard for infrastructure
- TIA 607-B, a generic standard for bonding and grounding for customer premises
- TIA 862-B, the standard for Building Automation Systems cabling

The Common Standards are further organized by user infrastructure type:

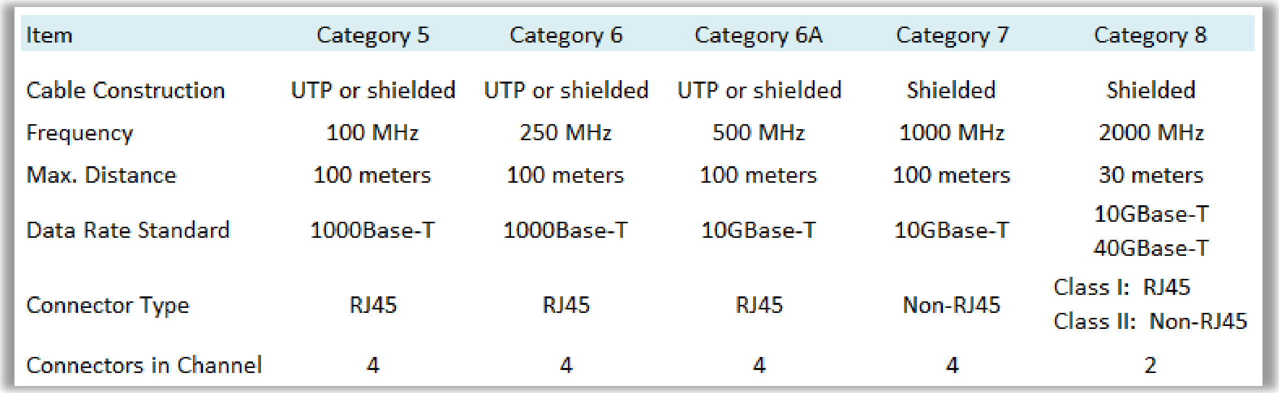
- TIA 568-C.1 for commercial buildings cabling
- TIA 570-C for residential infrastructure
- TIA 758-A for customer-owned outside plant cabling
- TIA 942-A for data centers
- TIA 1005-A for industrial premises

Supporting Component Standards:

- TIA 568-C.2 for balanced twisted-pair cabling
- TIA 568-C.3 for optical fiber cabling components
- TIA 568-C.4 for broadband coaxial cabling and components

Network structured copper cabling can be Category 5/5e and 6 unshielded twisted pair, or Category 7 and Category 8 shielded twisted pair types. Their respective properties and performance are shown in Table 13-2.

Table 13-2. IEEE Structured Cabling Properties



Item	Category 5	Category 6	Category 6A	Category 7	Category 8
Cable Construction	UTP or shielded	UTP or shielded	UTP or shielded	Shielded	Shielded
Frequency	100 MHz	250 MHz	500 MHz	1000 MHz	2000 MHz
Max. Distance	100 meters	100 meters	100 meters	100 meters	30 meters
Data Rate Standard	1000Base-T	1000Base-T	10GBase-T	10GBase-T	10GBase-T 40GBase-T
Connector Type	RJ45	RJ45	RJ45	Non-RJ45	Class I: RJ45 Class II: Non-RJ45
Connectors in Channel	4	4	4	4	2

Source: TranSecure, Inc.

Category 5e cable was introduced in 1999. Category 5e, 5, 6, and 7 types have been limited by the 100-meter, 4-connector channel baseline specification. The need for faster data rates has resulted in Category 8 cabling, which departs from this specification by using a frequency of 2000 MHz, and a 30-meter 2-connector channel. It will also require shielded cabling.

13.2.9 Telecommunications Rooms

Design of all telecommunication rooms, termination closets, wire rooms, and other components of the passive infrastructure should use short and direct lines as much as possible, to minimize cable run length. In multilevel buildings, efficiency suggests stacking telecom rooms to minimize the distance and labor in making connections among them. However, this may create a limited single point of failure that may be contrary to good security, e.g., if a fire in an upper level telecom room leads to water damage on floors below. In any case, telecommunications rooms should be established to support the BICSI and ANSI/TIA/EIA–568B requirements that no end device is located more than a 90-meter cable run from a telecom room to provide adequate coverage for both planned and future applications. This is important to note, as certain situations require that the routing of the cabling be performed in a less than direct route.

The size of the telecom room should provide sufficient working space for maintenance personnel, and enough room to accommodate all reasonable future expansion requirements. This should include panel space for cable terminations, switches and relays, remote field panels, remote diagnostic and management computer stations, and power service with redundancy and/or emergency back-up capability.

In designing telecom rooms, special consideration should be given to:

- Providing adequate clearances and space for access to the equipment; work space should be allocated for infrastructure operating staff and system administrators, and a small maintenance and spare equipment storage area also should be included
- Using multifactor access controls and incorporating unique user biometrics to prevent unauthorized access
- Sizing HVAC equipment to support typical heat loads generated by communications equipment
- Sizing a local UPS to power equipment in the event of a power failure; access to these rooms should be controlled

Telecom rooms that require tenant access should have a clearly defined tenant area that is access controlled. Planners should consider installing physical barriers that provide separation; rack configurations that limit accessibility; locking colocation cabinets that provide locking mechanisms for tenants as well as owner cabinets; and other appropriately restrictive measures.

13.2.10 Infrastructure Management

Cabling management includes the process and standards by which cabling and cabling infrastructure systems are installed, maintained, assigned, and labeled, both initially and throughout the lifespan of the systems.

Airports should take the earliest opportunity to design a cabling management plan. This plan should include standards for type of cable, how and where cabling is routed and its related infrastructure is installed, and standards for labeling, such as color-coding or other identification methods. The cabling management plan should also discuss assignment of cabling for each individual system's use, and a Conduit Plan that documents the origination and destination of all conduit runs within the facility. This is not merely an early planning function, but should be maintained for all ongoing changes throughout the entire life cycle of the system.

Among the issues of cable infrastructure labeling is the determination of whether to identify security cabling/infrastructure as such. This is an airport decision, but should be made in consultation with the Federal Security Director and first responders. There are degrees of identification, such as identifying security cabling/infrastructure only within Secured Areas or equipment rooms, or using coded identification that does not immediately imply security (i.e., red) to the uninitiated viewer.

Cabling labeling and installation should conform to Telecommunications Industry Association TIA/EIA-606A, *Administrative Standard for Telecommunications Infrastructure*.

Advantages of identifying security cabling through labeling include:

- Ease of identification reduces maintenance and repair times. Coding can identify cables to authorized maintenance and repair individuals without providing identification to the public or other unauthorized individuals. Cables are seldom in the public view; often hidden, they are typically above a dropped ceiling within a plenum space. Sometimes roof-mounted raceways and cable trays are used. Color-coding allows system identification without visually identifying the associated access point, communication line, or piece of equipment.

- Identification is valuable and can reduce costs when expanding, renovating, or modifying systems and/or architectural areas. It helps prevent accidental damage or cable cutting by installers and maintainers of adjacent systems.

Disadvantages of visually identifying security system passive architecture include:

- Use of identification can direct vandals or saboteurs to critical systems more easily.
- Use of coded identification or generic labeling of security systems/infrastructure can be misleading, which may be good for protection against vandalism and sabotage, but can cause installation and/or maintenance errors.

13.2.11 Cabling Infrastructure Systems and Management

Cabling infrastructure systems are composed of the structures by which cabling is contained, protected, secured and/or routed from point to point. Elements within cabling infrastructure include conduit, boxes, cable trays, and the various means of grouping, separating, routing and isolating cabling.

Cabling management maintains the system and standards by which cabling and cabling infrastructure systems are installed, maintained, and labeled, both initially and throughout the airport's lifespan.

With the variety of users and levels of service required at an airport, it is critical to use and maintain a consistent cable documentation system. There are several commercially available programs that track and document the cable infrastructure of facilities. Redundant infrastructure may be added for different users if there is no centralized control of the cabling structure within the facility. As various users, such as LAN systems, concessionaire point-of-sale systems, and security equipment, compete for airport cable bandwidth, spare fibers and conduits will be used on a first-come-first-served basis in the absence of centralized, thoughtful management and control.

13.2.12 Mobile Remote Display Units

The network infrastructure should also support mobile access to video imagery. Airport security response personnel are typically not in the SOC when an event happens. Being able to see what is happening on a portable digital assistant (PDA), mobile phone, or laptop—and having two-way voice communications to personnel at the event is an excellent capability, so that mobile users remain connected to the SOC and are aware of events as they unfold and can develop an appropriate response en route.

13.2.13 Network Availability and Accessibility

Networks supporting mission-critical communications should be highly reliable and available. In the presence of equipment and cable faults, such as power outage of network switches and broken cables, the network should be designed to continue without interruption. To ensure high network availability, airport design and construction should take into account the potential for network fault tolerance and resiliency, specifically:

- Dual or multi-network cabling to interconnect mission-critical computing equipment and platforms. The dual/multi-network cables can be physically routed along diverse paths to minimize the chances of being damaged simultaneously.

- Redundant network equipment, such as repeaters, switches, routers, and power supplies, should also be considered. Separate wiring closets may be allocated to host the redundant equipment (as physical distance limitations allow), and should be placed far enough apart to reduce the chances that all the equipment will be damaged in a single destructive event.
- The use of Power Distribution Units, alternate sources of power from different substations, and other redundancies helps to mitigate power outage problems. (Dual corded devices fed from the same substation may protect against accidental disconnection of a power cord, but offer little or no protection against local or regional power-outages.)
- UPS power should be utilized in each Main Distribution Facility and Intermediate Distribution Facility room, and should have a designed capacity for at least 25 percent future growth. Coupled with the use of line-powered CCTV, loss of access control power need not violate the integrity of the terminal security system.

Computer system designers routinely consider protection from failures and attacks, and often provide for both a primary application server and an online backup server. A third computer room may also be considered, containing “dark” backup servers that could be brought online if both the primary and backup servers are damaged. Network cabling to support such a room should be considered.

If implemented, dark servers should have a different virus protection and security scheme than the primary and backup computer systems, and their data should be updated daily after a 12-hour wait time with backup tapes from the primary server. A separate internet-access work station located in the dark server room provides a method of researching and downloading a security patch or virus protection data file.

UPS backup power requirements for IT systems typically are specified for several hours, on the assumption that standby generators or other sources will come online to provide power within that period. UPS for physical security systems, however, should be specified for worst case conditions that could extend a day or more, on the assumptions that alternative backup means may not be available or may not be able to carry the emergency loads. It is important that IT and security departments address this issue and agree on what will be provided.

Network architecture should include the appropriate meshed configuration to provide multiple routes between network components in the event of equipment or cabling failures.

WAN connectivity may be among the design considerations for internet and/or Virtual Private Network (VPN) access. The network design (including cabling) should take into account the need for WAN connectivity, security, and situations in which the airport provides shared networking services among different users, such as airlines, airports, concessions, and government organizations.

Many large and medium airports have installed a shared communications network to achieve high QoS levels and high system availability rates, which are particularly useful if airport operators expect tenants, airlines, and the TSA to share the network.

In most cases, airports have established a security systems network that is physically separate and distinct from the airport network used for the traditional operational systems. With the improvement of communications technologies such as VPNs and network security features, airport operators are now hosting security systems and related applications on the shared airport network.

There are pros and cons of sharing versus not sharing the networks, but those discussions are beyond the purpose of this guideline. It is recommended, however, that all relevant stakeholders (operations, engineering, IT, security, and, if applicable, the TSA), agree on their mission and system requirements, and determine which solution is best for its application. This is typically laid out in the initial ConOps.

13.2.14 Information Storage

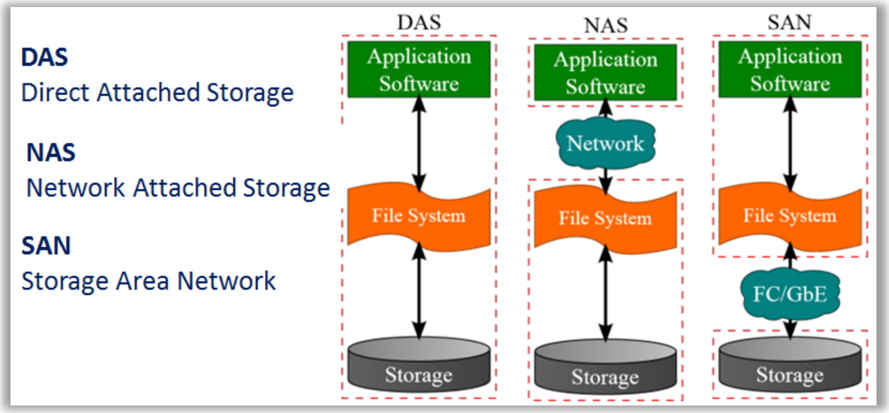
For many airport networks, the storage driver will be storing video imagery from surveillance cameras. Deciding on the amount of storage needed and the proper storage architecture will depend on evaluating:

- Camera array size (number of pixels)
- Encoding – constant or variable bit rate
- Compression – quality vs. transmission bandwidth
- Storage strategy – full video vs. motion-only video, and frame rate
- Storage duration – should be decided during the ConOps process

Storage systems for mission-critical file servers and databases should be highly reliable and available. In the event of equipment faults, such as disk malfunctions and power outages, the storage system should continue to function, taking into account redundancy and back up.

Storage redundancy may be achieved by mirroring storage devices in different locations via local area networks, using Redundant Array of Independent Disks (RAID) techniques, Storage Area Network (SAN) techniques, or Network Attached Storage (NAS) techniques illustrated in Figure 13-3 and Table 13-3.

Figure 13-3. Basic Features of DAS-NAS-SAN Storage Architectures



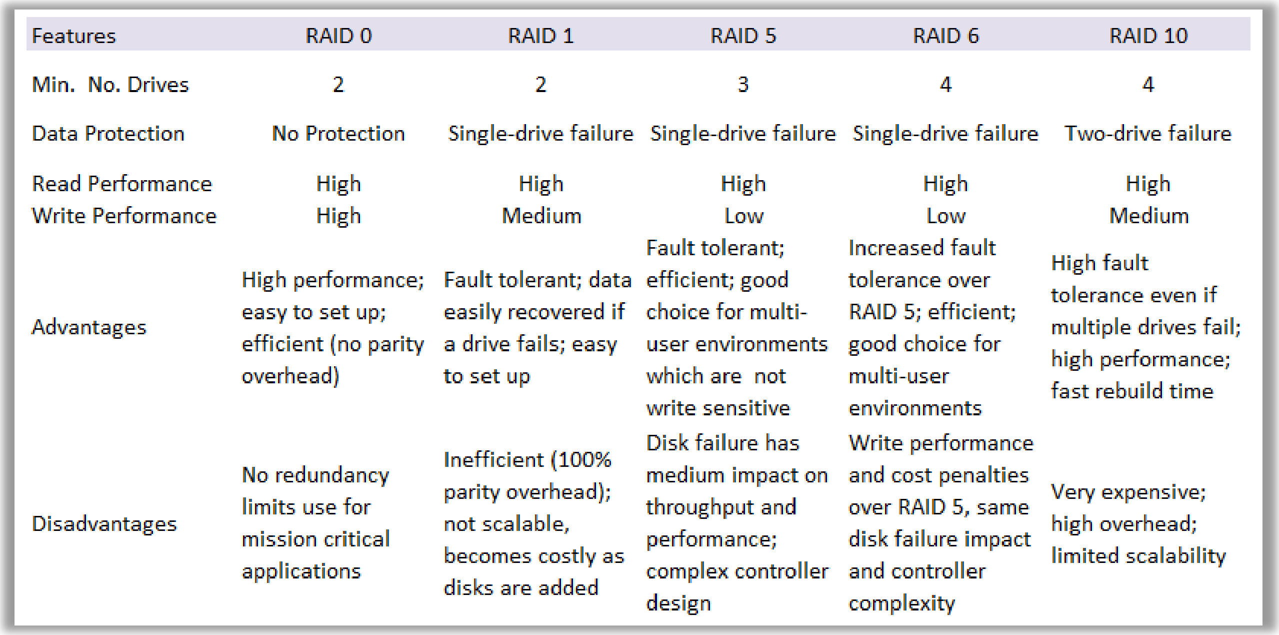
Source: TranSecure, Inc.

There are many more RAID configurations possible than are shown in this table, including custom configurations. Selection depends on the value and criticality of the data to be stored; the amount of data to be stored and the storage duration; the levels and location(s) of redundant drives and the provisioning of hot-swappable spare drives in RAID chasses; rebuild times, which for large arrays can be lengthy; drive maintenance; and, of course, cost. The first step in this process should be defining what is needed during the ConOps.

Each brings its own advantages, limitations, and costs. DAS is simple and low cost, but its functionality is limited. NAS is a common, cost-effective choice for medium sized networks. SAN is best suited to large networks and datacenters.

Disk storage costs have dropped to the point that terabyte disks can be inexpensively provisioned for many applications. Solid-state storage is trending in the same direction, but to date has been mostly limited to modest PCs and portable devices such as laptops and tablets.

Table 13-3. RAID Options



Features	RAID 0	RAID 1	RAID 5	RAID 6	RAID 10
Min. No. Drives	2	2	3	4	4
Data Protection	No Protection	Single-drive failure	Single-drive failure	Single-drive failure	Two-drive failure
Read Performance Write Performance	High High	High Medium	High Low	High Low	High Medium
Advantages	High performance; easy to set up; efficient (no parity overhead)	Fault tolerant; data easily recovered if a drive fails; easy to set up	Fault tolerant; efficient; good choice for multi-user environments which are not write sensitive	Increased fault tolerance over RAID 5; efficient; good choice for multi-user environments	High fault tolerance even if multiple drives fail; high performance; fast rebuild time
Disadvantages	No redundancy limits use for mission critical applications	Inefficient (100% parity overhead); not scalable, becomes costly as disks are added	Disk failure has medium impact on throughput and performance; complex controller design	Write performance and cost penalties over RAID 5, same disk failure impact and controller complexity	Very expensive; high overhead; limited scalability

Source: TranSecure, Inc.

13.2.15 Future Rough-Ins/Preparations

Comprehensive early planning can significantly reduce future construction costs. For example, where it is known that a future terminal expansion, additional concourses and/or gates, new buildings, or expanded or relocated security screening points may be built in the future, it may be prudent to include sufficient conduit, pull strings, cable or fiber, terminations, shielding or other rough-in elements to those locations during an earlier construction job. This helps avoid future need to tear up and repair walls or floors, dig trenches, and pull cable.

13.3 Wireless Systems

The three types of wireless systems that are likely to be useful for airport security are:

- Radio frequencies that are licensed to the airport by the Federal Communications Commission (FCC)
- Radio frequencies that the FCC has ruled may be used without a specific license
- Optical frequencies, which are not licensed by the FCC

The choice of wireless systems depends on the nature of the communications, including its required reliability and security. Applications that are considered by airport security to be mission critical should be provided with the maximum possible reliability and security. Reliability and security for other types of communications, including tenant communications for which the airport may legitimately exercise control, will still be needed, but the extent can be tailored to the user and the function being performed.

Obtaining a radio frequency (RF) license from the FCC should involve a specialist, such as an engineer or regulatory attorney, to assure that the process is completed without delays. If the FCC is receptive, a license can often be obtained in less than 60 days when properly prepared, but obtaining a license is never guaranteed.

13.3.1 Regulations

FCC regulations prescribe specific ranges of frequencies for different kinds of equipment. The FAA's Spectrum Assignment and Engineering Division (ASR-100) operates the automated Frequency Management System, the Airspace Analysis Model, and the Radio Frequency Interference Program. ASR-100 may be helpful in working though spectrum allocation issues associated with a RF telecommunications design at an airport. Key design decisions include antenna placement, cables and routing, and whether some functions might remain hard-wired.

The FCC has set aside several frequency bands for unlicensed wireless operations. The most popular commercial bands are the Part 15 Subpart C, known as the ISM band (for Industrial-Scientific-Medical users) and the frequencies set aside for WLANs, known as the Part 15 Wi-Fi bands. They are power-limited to minimize interference, which means limited range that can be overcome with high-gain antennas.

13.3.2 Radio Frequency Communications

When RF-based communications are adopted for an airport environment, their design should address the following issues at a minimum:

- Is RF-based communication the most efficient and cost-effective way to accomplish the necessary tasks?
- Will RF-based communication require unique infrastructure support not necessary with other modes of communication?
- Will airport RF systems interfere with other operational elements, including aircraft and air traffic communications, security operations, or general administrative data transfers?
- Will they operate in all, or at least the necessary portions of the terminal and grounds?

To answer these questions, the designer should consider the sources of RF and the systems that might be affected by targeted or random RF emissions.

13.3.2.1 Environmental Considerations

Environmental considerations that may be potential sources of interference for RF include:

- Cell phones
- Licensed and unlicensed equipment
- Metal detectors
- X-ray machines
- Explosive detection systems
- Advanced imaging systems

- Portable devices (pagers, PDAs)
- Power generators
- Power lines
- Power transformers

The physical environment can affect RF communications, depending primarily on the frequencies used, and, to a lesser extent, on the communications protocols. Relevant environmental variables include:

- Dust and dirt
- Rain
- Snow
- Temperature

13.3.2.2 Installation Considerations

Once the suggestion has been made to implement RF communication capabilities, numerous engineering aspects should be considered to determine whether the operational benefits will outweigh the installation and continuing maintenance costs, as well as the potential liabilities inherent in the possibility of interference. These include:

- Antenna: Location, mounting, and directional/omnidirectional considerations
- ATC communications interactions and interference
- Coverage areas (and dead spots)
- Mobile or portable
- Obstructions
- Other co-located or local transmitters, including those external to the airport, that have the potential to interact with airport RF communications systems
- Robustness of link
- Shielding, electrical interference (rebar, reflective insulation)

13.3.3 Wireless Standards

IEEE 802.11b is the original Wi-Fi band, later expanded under the “g” standard for higher data rates and lower dropped-packet rates. IEEE 802.11g was the third modulation standard for WLANs. It works in the same 2.4 GHz band as 802.11b, but operates at a maximum raw data rate of 54 Mb/s, and 802.11g hardware is fully backwards compatible with 802.11b hardware. Higher throughput is achieved by a more efficient modulation scheme, and to reduce susceptibility to interference, there are only three non-overlapping usable channels in the United States with 25 MHz separation. Even with such separation, some interference due to side lobes exists, though it is weaker than for “b” signals. This band is also shared by other emitters including Bluetooth devices, cordless telephones, and microwave ovens—all potential sources of interference.

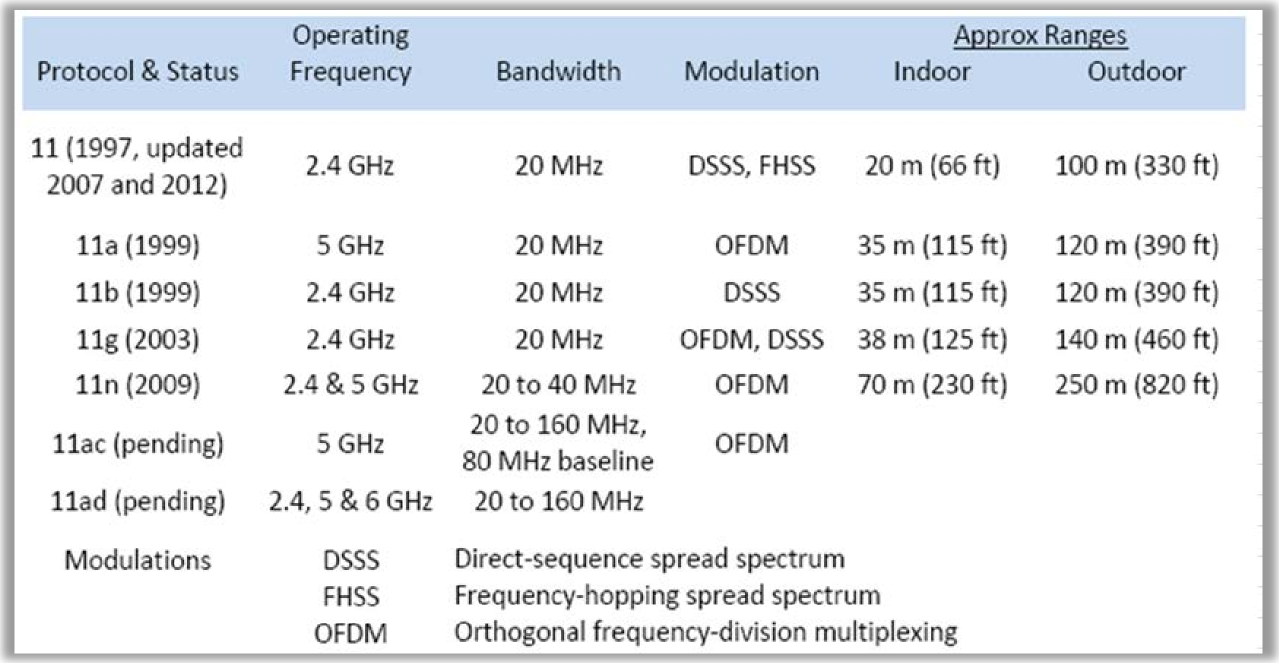
The IEEE 802.11a band improves on the 802.11b/g standards and also provides for operations in an alternative, possibly less congested band, with over three times the operating bandwidth in the 2.4GHz band with less susceptibility to interference.

The IEEE 802.11a band has 12 non-overlapping channels, 8 dedicated to indoor and 4 to point-to-point applications. The 8 indoor carriers are spaced across 200 MHz in the lower spectrum (5.150–5.350 GHz) and 4 point-to-point carriers are spaced across 100 MHz in the upper spectrum (5.725–5.825 GHz). The channels are spaced 20 MHz apart, which allows for high bit rates per channel.

To provide still higher throughput in WLANs, the IEEE developed 802.11n, which enhances operations in the 802.11a/g bands. The throughput can exceed 100 Mb/sec in 20MHz to 40MHz of bandwidth, and enables interconnection distances of 300 feet or more by using multiple antennas to coherently resolve multi-pathing data streams, where streaming video, such as the output of surveillance cameras, can require throughputs of 100 Mb/sec and higher.

Table 13-4 summarizes the properties of the available Wi-Fi bands.

Table 13-4. Properties of Wi-Fi Wireless Bands



	Operating			Approx Ranges	
Protocol & Status	Frequency	Bandwidth	Modulation	Indoor	Outdoor
11 (1997, updated 2007 and 2012)	2.4 GHz	20 MHz	DSSS, FHSS	20 m (66 ft)	100 m (330 ft)
11a (1999)	5 GHz	20 MHz	OFDM	35 m (115 ft)	120 m (390 ft)
11b (1999)	2.4 GHz	20 MHz	DSSS	35 m (115 ft)	120 m (390 ft)
11g (2003)	2.4 GHz	20 MHz	OFDM, DSSS	38 m (125 ft)	140 m (460 ft)
11n (2009)	2.4 & 5 GHz	20 to 40 MHz	OFDM	70 m (230 ft)	250 m (820 ft)
11ac (pending)	5 GHz	20 to 160 MHz, 80 MHz baseline	OFDM		
11ad (pending)	2.4, 5 & 6 GHz	20 to 160 MHz			
Modulations	DSSS	Direct-sequence spread spectrum			
	FHSS	Frequency-hopping spread spectrum			
	OFDM	Orthogonal frequency-division multiplexing			

Source: TranSecure, Inc.

13.3.4 Wi-Fi Bands

Although the Part 15 Wi-Fi bands are governed by IEEE standards, they are public, which means they can be used (and monitored) by anyone within the FCC-specified power/bandwidth envelope and antenna beam restrictions. They can also be saturated with public users. The rated distance assumes a single user, and adding one user could drop the range in half depending on the bandwidth of the transmission, i.e., video vs. text. The only protection from interception is encryption; there is no practical protection from saturation.

Wi-Fi systems are generally considered to operate over relatively short ranges because of FCC restrictions on radiated power, and because, as a shared medium, as the number of users increases the range for all users decreases. With the proper equipment, however, video transmission over ranges of 20 miles or more have been demonstrated.

Many airports already have 802.11 WLANs installed, either by airport management or by airport tenants. Since these WLANs operate in unlicensed bands, any user can install equipment that meets FCC standards for transmitted power levels. The proliferation of this equipment, and the resulting potential for mutual interference, poses a challenge for airports in view of the FCC stance that it alone can regulate radio operations.

Airport operators can seek to limit interference through voluntary agreements with tenants, who face the same problems, and can also restrict tenants from attaching Wi-Fi antennas to airport property; but under existing FCC rulings, airports cannot otherwise prohibit a tenant from operating Wi-Fi equipment.

Since it is difficult, and in some cases impossible, for airports to control Wi-Fi operations, using Wi-Fi frequencies for airport operations requires special attention to what functions should be permitted over wireless links and how to secure them over the network. Most video surveillance imagery is time-perishable, in which case transmitting it without encryption may be permitted if the network is adequately secured. That will not, however, protect such transmissions from interference. In principle, video imagery and other security information that must be delivered should not use the Wi-Fi bands. However, if an airport and its tenants can agree to reserve the 802.11a band solely for airport use, this problem can be mitigated.

13.3.5 Radio Frequency Identification Devices

Radio Frequency Identification (RFID) tags and other RFID equipment are entering use in the airport security system. In some airports, RFID is already used to track selected bags in the inspection process, and in air cargo. Standards for RFID tags are not mature at the time of this writing. One standard would use RF in the 13.56 MHz range; another in the 2.45 GHz range. The latter range is available for unlicensed use within the United States, and is currently the frequency range of choice for a number of commercial WLANs appearing in airline lounges and in use by some airlines for bag system bar codes. As a result, care should be exercised in locating RF tag scanner equipment, to prevent interference from other sources. Shielding and physical separation, together with an RF spectrum survey of the airport, should be considered.

Antenna Pointing and Equipment Placement: Antenna pointing and interference issues are strongly related to the choice of systems. In general, higher frequency systems tend to have more directional antennas; hence their radiation emission and susceptibility can be better predicted and controlled. Also, the RF environment outside of a physical building is much more unpredictable, so efforts should always be taken to isolate as much as possible the internal and external environments. Choke Effects: At the lowest frequencies (such as generator resonance, etc.) wavelengths are very long and may be matched to terminal openings such as passageways for baggage handling equipment. Interconnection of subsurface metallic rods, building I-beams, and the metallic pillars and beams that surround openings can create an effective RF choke, helping to contain, ground, or dampen device interference at these frequencies.

13.3.5.1 Near Field Communication

Near field communication (NFC) is a set of standards for smartphones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimeters. NFC standards are based on existing RFID standards. NFC-enabled smartphones are already being used at airport check-in kiosks and at gates to check boarding passes.

13.3.6 Optical Transmission

Optical wireless systems use laser beams to carry video and other information. These are usually point-to-point systems. An optical beam is very narrow and cannot be detected or captured by radio receivers. Optical wireless systems also generally transmit in the infrared band, so the beams are not visible to the naked eye. These features make optical wireless difficult to intercept and attractive for secure transmissions.

On the other hand, the reliability of optical beams depends on the quality of the atmosphere. Rain, snow, fog, and sandstorms can degrade a link or even cause it to fail. This is a function of the link margin, i.e., the power of the received beam over the transmitted distance compared to atmospheric losses. For many environments, at the level of service required for security systems (equal to the telecommunications service level of 99.999 percent), optical transmission links are only candidates for relatively short distances. If there is uncertainty about the optical link performance, it should be tested under the local environmental conditions of worst-case concern before a commitment is made to use such equipment.

13.4 Information Assurance

Issues regarding Information Assurance include the process of detecting, reporting, and responding to cyber threats. These considerations include both design and procedural issues.

Eavesdropping or interception, as well as corruption of both content and control of data, are security threats when the data or their communication infrastructure (over the air or cables) are accessible to unauthorized persons. This can be addressed in the planning stages by such things as the placement of wiring or conduit in protected routes; placement and orientation of antennae; or encryption of data. Cybersecurity is addressed greater detail in Section 14.

13.5 Physical Protection of IT Assets

Physical security of network assets, including cable terminations installed in telecommunications rooms, should be addressed during system design, and include facility vulnerability to external explosives, required level of security, access means, and the granting and control of access privileges.

If the Physical Access Control System uses biometric smartcards for access to Secured Areas of the airport, at least the same level of access security should be adopted for telecommunication rooms.

If third-party equipment is installed in telecommunications rooms, the airport’s network equipment should be isolated by floor-to-ceiling cages of steel chain link mesh, and so should the equipment of each third party. Access card readers should be provided for each area, with only airport security and airport IT personnel having access to all third-party cages.

13.6 Electrical Power

The airport should assess potential impact of power outages on the availability and integrity of security, communications, operations, and emergency egress systems. Assessment should consider the need for low voltage devices and control systems, battery-driven remote and stand-alone devices, standard 110/220 voltage for operating equipment such as lighting and CCTV monitors, and high amperage/high voltage systems for such things as explosives detection systems and other screening and security equipment.

In providing redundancy or backup, the designer should consider the location and capacity of standby generators, and installation of redundant power lines to existing locations, as well as to alternate locations where emergency conditions might cause shifts in operational sites. In addition, strong consideration should be given to the installation of power lines, or at least sufficient conduit and pull-strings, to known future construction locations such as expanded terminal concourses.

When planning and reviewing utility services, 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) are desirable capabilities 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 assure protection of the security system and data network from damage resulting from loss of power.

If possible, the power source for a building should be from two separate sources, such as an emergency diesel generator system connected to the emergency (bus) distribution system. Use of automatic transfer switches is required to achieve automatic shift to the emergency power source. Electrical system architecture should be evaluated to provide the greatest uptime and availability through the use of maintenance arrangements, UPS, and battery backup systems.

The “cleanliness”—that is, the freedom from amplitude and other fluctuations of electricity on the power line—should not be assumed. The high concentration of harmonic generating loads at an airport may contaminate power flowing through airport lines. Use of proper grounding is vital; harmonic mitigation should be considered. This can include the use of phase-shifting transformers and UPS to provide a clean sine-wave to sensitive electronic loads. (The use of K-rated transformers does nothing to correct the harmonics on an electrical system; it merely generates more heat that the HVAC system must handle.)

Systems such as 400 Hz aircraft ground power units and chargers for electric ground service equipment should be isolated and fed from dedicated sources if possible.

Backup power for lighting is required for life safety systems; many options that are allowed under local building codes raise security considerations.

- Generators are the most common form of emergency backup; however, most local building codes require generators to come online up to 10 seconds after loss of power. This means that the building will be dark during this time period and potential security breaches may not be detected.
- Lighting supplied with integral battery packs are a maintenance item and provide less than full-power lumen output on the lamps that they control. Battery packs should be tested on a monthly basis, as they have the potential to fail if not properly maintained.

- Lighting inverters offer the advantage of providing immediate full lumen output upon loss of normal power, are easily maintainable, and can control large areas from the security of an electrical room. In addition, if properly specified, these units may be used to backup high-intensity discharge-type light fixtures that provide lighting for larger areas.
- Egress lighting level should be one footcandle in the path of egress. Most cameras will record down to 0.5 footcandles; however, the level of detail that can be distinguished is greatly reduced. Properly applied emergency lighting in critical areas is crucial to maintaining the integrity of the security and surveillance systems.

Integration of the security system with life safety systems is critical. Both the Uniform Building Code and the International Building Code require all locked doors in the path of egress to be unlocked whenever an event, such as fire alarm pull station activation, has occurred. Coordination with the local jurisdiction is critical to design without jeopardizing the safety and security of building occupants. Requiring the manual initiation of a pull station to open an exit door, and interlocking all doors in that egress pathway only, is a conceptual approach to this requirement. This is particularly important to counter use of a fire alarm activation as a diversion, which could enable access to restricted areas and/or the AOA. Automatic security camera call-ups, segregation of alarms within a building to alarm only the zone of incidence, and activation of a warning to adjacent zones all increase the likelihood that a secure perimeter can be maintained during an emergency.

The security of the power sources with regard to airside/landside placement, controlled access, and vulnerability to intrusion also should be considered, including the physical security of access portals.

Due to the increasing deployment of IP-based CCTV cameras, Power over Ethernet (PoE) technology is becoming a readily available power source. PoE is advantageous to deploy in applications where UPS is unsuitable and where AC power would be inconvenient, expensive, or infeasible to supply. However, even where UPS or AC power could be used, PoE has several advantages over Ethernet, including less costly cabling, higher bit rate support, direct injection from standard 48-V DC battery power arrays, and symmetric power distribution.

13.6.1 Electrical Grid Dependency

Most airports depend on external grids for their electrical power, which are operated by municipalities and/or may be privately-owned. During the ConOps development, planning and design should include provisions for backup electrical power sized for emergencies and outages. It should also provide for alternative power feeds if the area is served by more than one utility and provisions for routing power around substations in the area.

DHS has an active program to assist utilities and industrial facilities in securing their facilities against both physical attacks and cyber-attacks. DHS works through trade groups for water, power, chemical, and other industries, and has developed National Response Plans for all of them. The Department of Energy and its laboratories are also actively developing physical and cyber defense mechanisms for the industries under their governance.

Federal security measures include industry development of related security standards and best practices. As one example, the Federal Energy Regulatory Commission has mandated a reliability standard requiring electric utilities to protect their transmission facilities and control centers against physical threats. The standard directs electric utilities to perform risk assessments to identify the substations that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Transmission owners must also identify the control centers for those critical facilities; perform threat assessments to identify the physical threats and vulnerabilities to their facilities; and to implement physical security plans to address them.

For electrical utilities, the North American Electric Reliability Council has measures to assure a secure physical environment for cyber resources. This represents a minimum set of measures derived from commonly accepted industry standards and practices, such as the common criteria found in CTSEC, ITSEC, IPSEC, ISO 17799, NIST Guidelines, and the NERC Security Guidelines.

13.6.2 Trends

The reduction in cost of 10 to 40 GbE network equipment will encourage network design changes in at least two ways:

- Providing more bandwidth, additional security devices can be supported, especially megapixel video cameras.
- Flattening networks to minimize latency (jitter) and other aspects of QoS, as well as lower equipment and maintenance costs. The exponential growth of mobile devices, especially smartphones, will further integrate mobile security personnel into SOC functionality and enable many SOC functions to be performed by mobile users, if the appropriate procedures to do so are in place.

Communications interoperability across diverse networks continues to be an elusive goal, but recent developments are encouraging and, with appropriate planning and coordination, communications interoperability is now possible.

Networked communications will only be effective if they are also secure, not just in transmission, but also hardened against hacking and cyber threats. This is discussed further in Section 14.

13.7 Checklist

Communications, IT, Power, & Cabling Checklist

☐ Develop operational requirements using the ConOps process
- ▪ Determine SOC requirements
- ▪ Identify networking requirements
- ▪ Identify physical space limitations
- ▪ ID video storage requirements
- ▪ Determine legacy system replacements
- ▪ Identify allowable social media access
- ▪ Identify interoperability requirements

☐ Communications-IT-Power Planning and Design
- ▪ Establish network design objectives; scalability
- ▪ Identify standards to be applied
- ▪ Evaluate dedicated vs. common IT network
- ▪ Identify nodes/edge devices
- ▪ Determine bandwidth requirements
- ▪ Provide 100% growth potential for fiber

- For cabling links, use non-shielded cabling
- Assess QoS for wireless links
- Secure telecom rooms with biometrics
- Evaluate video storage alternatives
- Consider off-site cloud storage for non-critical data
- Establish redundancy and backup requirements
- Plan for expansion of Wi-Fi services
- Establish cybersecurity requirements

Detailed design information for the SOC applications, networking, communications, CCTV and supplementary functionality can be found in complementary sections throughout this document, as well as in industry and government guidance documents noted in the bibliography.

SECTION 14: INFORMATION SECURITY

14.1 Introduction

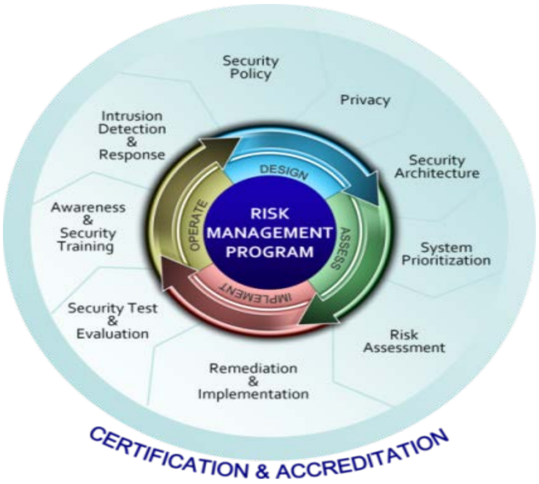
This section outlines planning and design considerations for protecting, detecting, and responding to attacks on the airport's IT network, including cyber threats and measures to guard against them. The aviation industry, and airports in particular, is highly dependent on IT for daily operations. IT systems are widely used as security platforms for airport access control and alarm monitoring systems, video surveillance systems, 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.

14.2 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. These steps are illustrated in Figure 14-1.

Figure 14-1. Risk Management Cycle


Security Policy
Privacy
Security Architecture
System Prioritization
Risk Assessment
Remediation & Implementation
Security Test & Evaluation
Awareness & Security Training
Intrusion Detection & Response
DESIGN
ASSESS
IMPLEMENT
OPERATE
RISK MANAGEMENT PROGRAM
CERTIFICATION & ACCREDITATION

Source: System Development Integration, LLC

Recurrent Steps of Cyber Risk Cycle

- Security Policy: Describe the organization's information protection and privacy objectives, as stated by management and in the ConOps
- 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
- System Prioritization: Develop a ranked inventory that identifies the organization's critical systems and sensitive data
- Risk Assessment: Conduct a threat/vulnerability/consequence/risk analysis 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 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 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, policy 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 access control systems to Secured Areas critical to the airport network.

Information security measures that airports should especially address in the ConOps are:

- 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 concessions, suppliers, and authorized visitors

Recent technological developments and moves to increase efficiency have resulted in the merging of traditional IT networks with Supervisory Control and Data Acquisition Systems (SCADA). However, SCADA systems often have vulnerabilities like hardcoded administrative passwords or non-securable ports and services. Airports often have homogeneous networks that are connected together with cybersecurity as an afterthought. This is a challenging and complex problem that introduces an additional set of vulnerabilities. IT staff can meet these challenges by employing in depth defense and network segregation practices to improve the security posture for SCADA and Building Automation Systems.

Additionally, the use of “Bring Your Own Devices” to create electronic boarding passes and other internet-based services has created a borderless network. The challenge facing airports is a constantly moving target of technological platforms that require the cooperation of multiple departments and disciplines across the airport to manage security effectively. During the planning process, IT staff should identify means of monitoring and controlling use of employee devices. They should also plan for segregating guest services like Wi-Fi.

14.3 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 unsecure 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

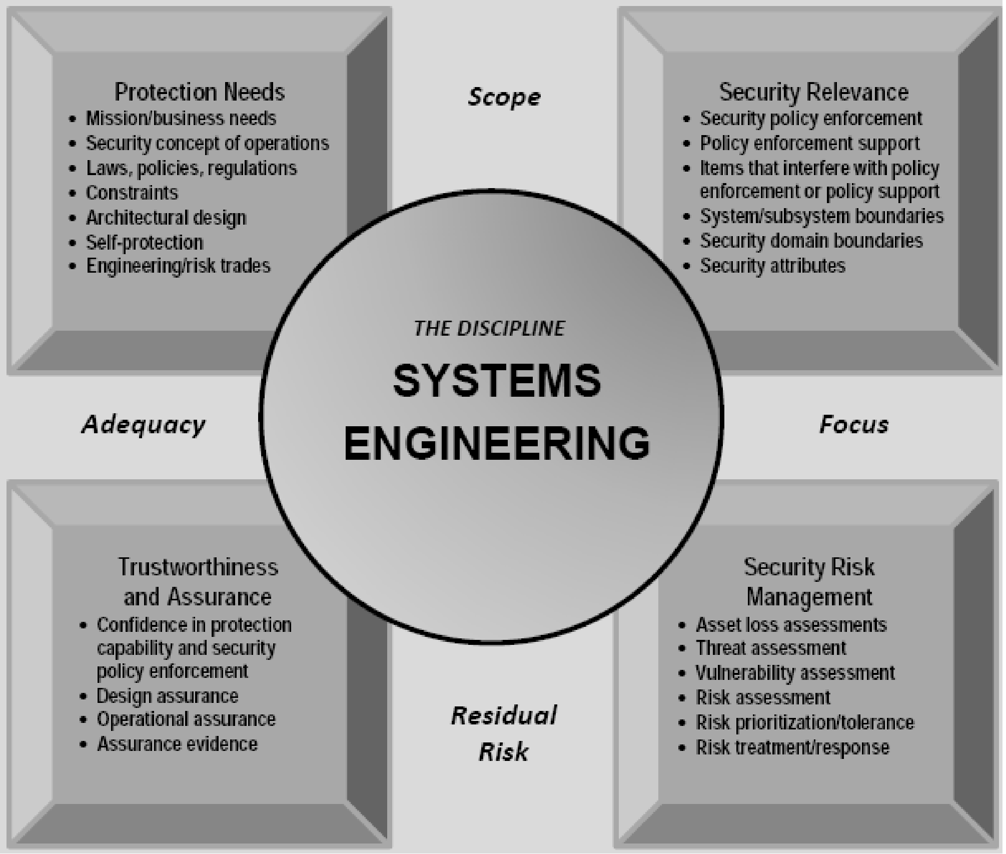
IT system designs at airports should include intrusion detection or intrusion protection systems, often functionality incorporated into firewall appliances. IT staff may also consider incorporating Data Exfiltration Protection functionality or appliances. The logs from these systems and the firewalls 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. Sample forms are found at DHS, ICS-CERT if the incident involves a SCADA or Industrial Control System, or the Center for Internet Security.

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.

In designing an IT system to meet such threats, the system's operational requirements (including information security requirements) should be identified first, preferably as part of the overall ConOps. Whenever selecting systems, it is important that security is built in rather than added later. The more complex an airport IT system is, the likelihood of "missing something" grows, thus opening up a potential vulnerability. Many modern airport IT networks link multiple critical systems, which are then supplied with data from several external sources, each of which can bring its own vulnerabilities. For this reason, it is critical that the airport IT planner/designer ensures that each connection is secure, protected by the appropriate firewalls, and that the data transmitted is appropriately encrypted.

NIST is developing guidelines to protect IT systems, particularly from cyberattacks. Special Publication (SP) 800-160, Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, is in its second public draft at the time of this publication, and is an excellent resource for airport IT security managers. SP 800-160 takes a systems engineering approach to security, as illustrated in Figure 14-2:

Figure 14-2. Essential Contributions of Systems Engineering



Source: NIST

NIST set out to include security considerations from original design throughout a system's entire life cycle, including how to retire a system and its data securely. The latest draft adds security concepts to critical non-engineering processes involving these systems, such as management and support services.

NIST's Risk Management Framework SP 800-53 can provide airport IT staff with a complete process for determining the risks of information systems, as well as the security controls to be applied to the systems based on risk levels.

14.3.1 System Architecture

Most airport physical 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), on the availability of skilled personnel, on facility characteristics such as cable plant paths, and on budgetary limitations. Selecting an appropriate architecture is an important issue to be addressed during the security system ConOps.

14.3.2 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 required.

14.3.3 Biometric Identification

Authentication based on physical characteristics is classified as biometric authentication; the most common include fingerprint readers, hand-geometry sensors, iris scanners, facial recognition systems, and voice identification. They can also be combined with passwords and tokens to establish a higher degree of trust than the use of a biometric reader alone.

A third authentication process moves away from explicit logins toward a more passive model, generally referred to as continuous, which monitors a user’s on-network experience (e.g., behavior, actions, and physical attributes that may include expected typing patterns, types of transactions, face geometry, and more) to assess the identity of the user.

From a planning and design perspective, adopting biometric identification depends on where and how the biometric functions are to be implemented. Biometric functions that use access cards require card readers and cabling to support them. Iris scanning presents similar issues. Facial recognition systems require cameras, but if they are able to utilize video surveillance cameras, the hardware and installation issues may be less demanding. Voice recognition systems require microphones and associated cabling, but again, if video surveillance cameras include intercom functions, then these applications are easier to implement. Being primarily software applications, biometrics such as facial and voice recognition are easily updated.

14.3.4 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. Most recently, publicized major attacks, such as Stuxnet and Sony Pictures, have been traced to either deliberate or careless use of flash drives. 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. But carrying tokens everywhere means that they can be stolen, and in a large enterprise, tokens are a nuisance to manage.

14.4 Legal Issues

The massive amount of data collected by a range of security systems, including access control or video, raises several legal considerations that can impact system planning and design. 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, and the safeguarding and dissemination of data. These requirements can vary significantly between jurisdictions, so a legal review of protections for the planned video system by airport counsel is recommended.

The legal issues generally fall into two categories: what information can be collected, and how that information can be used.

14.4.1 Eavesdropping

Eavesdropping or interception, as well as corruption of both content and control of data, are security threats when the data or their communication infrastructure (over the air or cables) are accessible to unauthorized persons. This can be addressed in the planning stages by such things as the placement of wiring or conduit in protected routes, placement and orientation of antennae, or encryption of data.

14.4.2 Data Collection

The principal concern with respect to data collection is privacy protections. The focus of an agency 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 with respect to protection of privacy is a privacy impact assessment to assess the need for the data collection, which, in the case of airport background clearances, 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 both federal and 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 CCTV operators to observe those areas by means such as restricting pan-tilt-zoom camera coverage or using software that blocks the views of concern.

Legal issues can also arise where CCTV 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.

14.4.2.1 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 the copying and disseminating of 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 ConOps. 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, including video 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 that necessary for detection, orientation, or recognition, which translates into higher resolution and costlier video cameras, lenses, and storage devices.
    - During ConOps 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 of video data to be used as evidence to ensure the integrity of that data.

14.5 Trends

Information security trends track both emerging technologies and new threats directed against them. As technologies evolve, this is likely to include greater use of artificial intelligence and the expansion of smart machines, including networked robotic machines, which in some cases can operate autonomously. It will also include widespread application of the Internet of Things, which seeks to connect everything everywhere over the internet, often with security measures in the cloud, which are maturing but still have significant risk issues.

Using the cloud for security data (i.e., moving toward a model that offloads routine functions to cloud servers) is a trend driven by economics and the burdens of maintaining complex IT systems. Several U.S. government agencies, including DHS, now use cloud-based services for administrative functions and are developing measures to assist non-governmental entities in securely using cloud services.

Another important trend in information security is greater use of multifactor, biometrically based authentication for anyone accessing the IT network from any point or node on the system, including external access from the internet and the attachment of portable devices such as flash drives. While this does not eliminate the insider threat from appropriately authorized individuals, it does considerably narrow the exposure.

DHS is working with industry on biometric processes that would enhance mobile security and eliminate the need for passwords. Under its Mobile Technology Security Research and Development Award, DHS will combine behavioral sensing and modeling techniques for user authentication. The project is based on technology from university research partners, and is similar to research being pursued by the Defense Advanced Research Projects Agency.

However, recent NIST research reports reveal a significant degree of uncertainty regarding the security of some aspects of two-factor authentication. On the technical side, multifactor biometric authentication goes a long way toward thwarting unintended threats, if it is used. Without security awareness training and management support, any technological solution is vulnerable.

Another trend regarding passwords is offered in NIST SP 800-63, which is awaiting government approval at this writing, and would provide guidance on moving away from complex and hard-to-remember nonsensical passwords (example: Dk17#$jK) because much legacy software was restricted to 8 characters, including a capital letter and a special symbol. The NIST proposal suggests longer, harder to crack, but easier to remember plain English “passphrases,” such as “My brother-in-law really hates broccoli!”

The insider threat is more behavioral than technical. On the behavioral side, in addition to awareness training, there must be diligent monitoring of user logons, site usage, and file storage and transfers; i.e., the user should have an internal function that looks for signs of threats, including unusual behavioral patterns.

14.6 Checklist

Information Security Checklist

□ Develop operational requirements using the ConOps process
- Threat and vulnerability assessment
- Cybersecurity requirements
- Prioritize IT resources
- ID interoperability requirements
- Involve IT department in all discussions

□ Information Security Planning and Design
- Establish multifactor authentication needs
- Consider multifactor access for critical areas
- IT security at non-network applications
- Requirements for redundancy and backup
- Establish cybersecurity requirements.
- Evaluate cloud storage for routine files
- Address legal and privacy issues

SECTION 15: SECURITY OPERATIONS CENTERS AND COMMAND & CONTROL

15.1 Introduction

A ConOps for the airport security system should establish the primary goals and the operational requirements for security systems and later upgrades. The next step is the detailed planning of the facility where security operations will be managed. This is usually known as the Security Operations Center (SOC), but other names and acronyms are often used when other functions are jointly performed there.

15.2 SOCs and Related Operational Facilities

An SOC is the focal point for airport security monitoring, command and control, and communications functions. These functions often involve SSI, dissemination of which needs special control. Generally, an SOC will be a 24/7/365 operation, staffed and designed pursuant to the guidance of the security ConOps and the Airport Security Program (ASP).

The SOC generally serves as a platform to collect information from a range of sources 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 should include the capability to coordinate of security functions with other operations, e.g., Airport Operations Center (AOC), Emergency Operations Center (EOC) and Incident Command Posts (ICP).

15.2.1 Airport Operations Center

An AOC focuses mainly on the day-to-day operations of an airport, including issues such as maintenance of the airfield; runway surface and lighting; the management of terminal facilities; and control over gate operations and aircraft maintenance areas (although some of these may be tenant functions). SOC design should support the ConOps for airport operations, including linkage to the SOC and EOC in the event of an incident, because many security events will profoundly affect the continuity of daily operations.

15.2.2 Public Safety Answering Points

Public Safety Answering Points (PSAP), also known as 9-1-1 centers, are charged with managing public safety personnel and response, such as police, fire, and emergency management systems. An airport PSAP can serve as the focal point for 9-1-1 service to a larger geographic area outside its fence, receiving and processing emergency calls and event notifications for a specific area. PSAPs should have the flexibility to include additional operators during emergency situations.

15.2.3 Emergency Operations Center

An EOC is focused primarily on managing emergencies. It is often not occupied until it is activated when an incident occurs. Technology infrastructure should be designed to accommodate unfamiliar outside users from multiple organizations, and should be scalable for the sudden influx of people when emergencies occur.

The EOC is a physical location at which information and resources support incident management and on-scene operational activities. It may be a temporary facility, or it may be located in a more permanently established facility, often near the SOC/AOC. It may be organized by major functional disciplines (e.g., fire, law enforcement, medical services), by jurisdiction (e.g., federal, state, regional, city, county), or by some combination thereof.

15.2.4 Incident Command Post

ICPs are field locations where primary security, police, and emergency functions are performed at or near the event. The ICP may be co-located with other incident facilities; co-locating multiple facilities can leverage infrastructure and reduce overall cost. It is sometimes desirable to co-locate two different types of command centers in the same facility. For example, having an EOC next to an AOC/SOC can have definite advantages during emergencies, allowing easier communications among emergency managers of other groups. Architectural approaches such as glass walls/doors or movable walls provide the flexibility to achieve collaboration without disruption. Glass walls can also allow visual communications between EOC and AOC/SOC staff, as well as enable sharing of visual resources like video walls.

15.2.5 Fusion Centers

Fusion centers are designed for the interaction of multiple organizations in a facility that encourages collaboration. Fusion centers are typically utilized by government agencies to collaborate on intelligence issues, and exchanging knowledge not easily communicated via more formal channels of communication. Multiple agencies can collaborate to provide resources, expertise, and information to the center with the goal of maximizing the ability to detect, prevent, investigate, and respond to criminal and emergency activity. The airport is usually a participant/user rather than the host agency.

15.3 Planning the Design

15.3.1 The ConOps Process

The ConOps will typically be generic and high level. As planning progresses, this preliminary schedule can be refined and formalized with a fuller identification of the tasks for planning, as well as design and construction requirements, milestones, and interdependencies. It will serve as the baseline from which future design and construction schedules can be periodically developed, refined, and amended.

Planners should choose an architect/engineer with experience in SOC facilities. There are many operational nuances unique to SOC facility design beyond the range of normal experience of most traditional architects and engineers. Many of the technology systems that support physical security efforts are monitored, and in some instances integrated, at the SOC. Project management is a key factor in a successful effort.

15.3.2 SOC System Concept

The configuration and functionality of the SOC will depend on its how its roles and relationship with responder dispatch and incident management functions are defined in the ConOps, and how the SOC is staffed and trained to perform these functions. At many airports, and particularly when 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.

15.3.3 SOC Configurations

A primary SOC is generally located within an airport's Secured Area with secondary (or satellite) locations identified for protected redundancy. The SOC general design considerations include sufficient space and support facilities for personnel and IT equipment to facilitate rapid access and dispatch. Secondary or backup 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. In seeking to attain situational awareness, 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. Ultimately, 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 a human SOC operator to synthesize multi-sensor data into the optimal response, making necessary adjustments in real time. To assist the operator in making optimal responses, CCTV 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 risks.

SOCs come in all sizes and configurations—there is no single best design. The examples below show different approaches to coping with size and functional requirements. There is wide variation in functionality, design, and sizing. Each SOC must be adjusted to local operational requirements and facilities, and to local budgets.

Most often associated with the AOC is an EOC, often in an adjacent room equipped with a large table having both power and Local Area Network (LAN) outlets for laptop computers, and large video screens to display activities occurring at multiple sites.

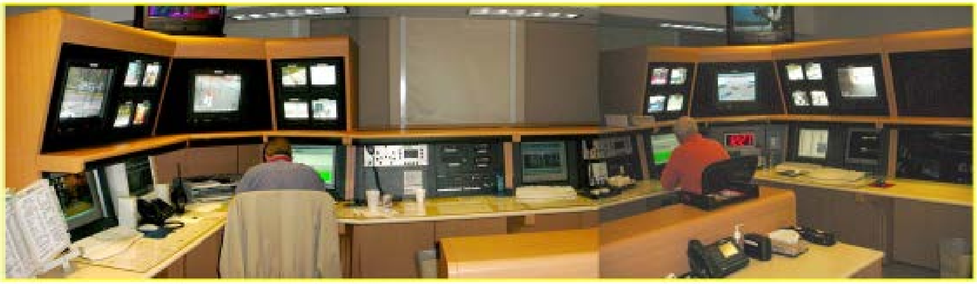
Communications modes and technologies typically include:

- Wired telephony, usually the primary communication with external parties
- 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

15.3.3.1 Small Airport

This airport (Figure 15-1) has an integrated SOC-EOC facility. The Airport Police Department is located separately, close to the TSA checkpoint, to facilitate rapid response to incidents. It operates as a stand-alone 24/7 facility, and is configured and equipped for redundancy of certain communications, IT, and power functions.

Figure 15-1. Small Airport SOC-EOC



Source: TranSecure, Inc.

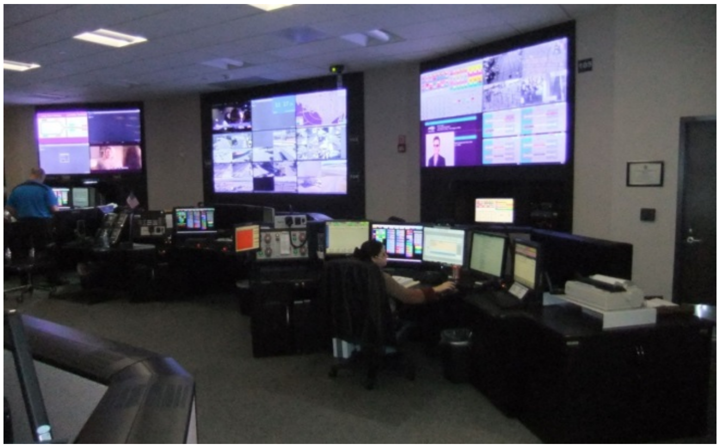
The airport SOC serves physical security functions (video surveillance, access control, etc.), supports airside and landside operations, and performs incident management, including fire incidents and area-wide emergency operations. Communications are complicated because portions of the airport are within multiple local jurisdictions and airport communications are not interoperable with one of them.

15.3.3.2 Medium Airport

This example (Figure 15-2) shows an integrated SOC-EOC-AOC Police Dispatch. The AOC provides Police Dispatch, surveillance and physical security monitoring, and emergency operations support functions, including response to physical attacks and natural disasters as set forth in the Airport Emergency Plan. Within the AOC, the multiple stations are equally capable, and operating personnel are cross-trained for their functions to provide local redundancy.

The AOC may contain a full set of communications modalities, including wired telephony, cellular telephony, 800 MHz trunked radio talk groups, and a LAN capable of carrying IP telephony. Mobile and portable radios can be programmed with the conventional talk-around channels used for car-to-car, portable-to-portable, and portable-to-mobile communications. In an emergency, these channels can provide communications between units working an event.

Figure 15-2. Integrated SOC-EOC-AOC-Police Dispatch

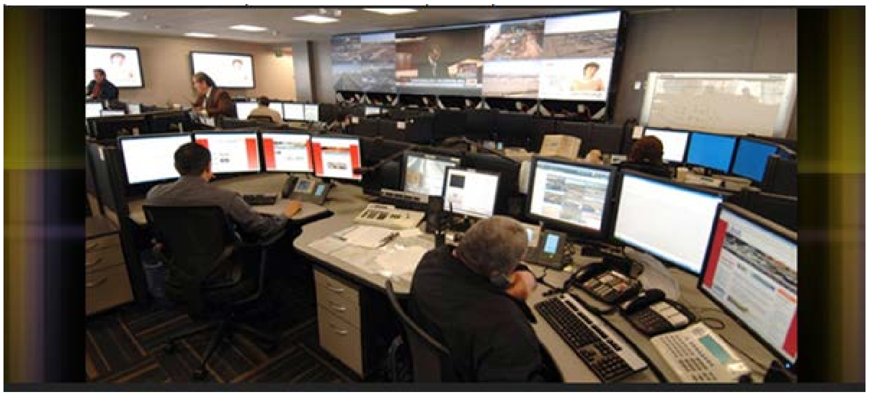


Source: TranSecure, Inc.

15.3.3.3 Large Airport

This integrated SOC-EOC-AOC (Figure 15-3), serves a large international airport. The design was driven by the airport’s Security Master Plan and an extensive ConOps to determine all operational requirements, with emphasis on using technology and response processes to support public safety operations.

Figure 15-3. Large Airport Integrated SOC-EOC-AOC



Source: System Development Integration, LLC

The ConOps for this airport’s security system upgrade considered a list of possible functions:

- Radio communication between the center, mobile airport personnel, and first responders
- 800 MHz trunked radio systems for interoperability with off-airport parties, including public safety agencies and fire departments
- Dispatch operations use a CAD system that includes integration of camera view into the dispatch process
- Using the access control system as the master log end event database, so that these functions do not have to be duplicated in video surveillance and other applications
- Extensive training of SOC personnel in situational awareness and the ability to address alarm and emergency situations

15.4 SOC Design

15.4.1 Design Objectives

The SOC design process should address the following performance and functional objectives.

15.4.1.1 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.

15.4.1.2 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 derived from 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 equipment design and manufacturing processes.

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.

15.4.1.3 Standards-Based Open Architecture

Open systems are those that conform to open specifications for interfaces, services, and supporting formats. An open specification or standard is a public specification that is maintained by an open public consensus process to accommodate new technology over time, and is consistent and compatible with existing standards.

15.4.1.4 Interoperability

Interoperability is a measure of how well one or more elements of the SOC and its technologies are able to work with other systems and components. Ideally, this should happen in a plug-and-play context (i.e., without having to modify electrical and mechanical interfaces or write software patches), and should be implemented using tested, proven open standards. Interoperability is primarily an issue of communications among system components.

15.4.1.5 Legacy System Integration

Most airport facilities have several existing systems and supporting infrastructure in place. The two most prevalent types of legacy systems are Physical Access Control Systems and Video Management Systems. These systems typically have well defined interfaces that allow access to system data. An SOC employs 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.

15.4.2 General Design Considerations

In most SOC development processes, it may be necessary to use the services of a qualified design team composed of architects, engineers, and specialty consultants (possibly including audio/video designers, acoustical engineers, and lighting designers). While many larger airports have internal resources with experience in some of these areas, few have extensive experience designing these complete facilities. The components and requirements of SOCs are complex and unique enough that specific expertise is essential.

This is not to say that internal staff should not be engaged. Indeed, architectural, engineering, and other design and operational professionals within the airport organization are the primary contributors of a user perspective to the ConOps, and have the locally specific experience and understanding of the unique environment to support the process. They should be involved from the early stages as stakeholders and active participants.

An SOC facility is not merely an architectural and engineering effort, but is at the core of airport security operations, interwoven into the operational systems. The technology must work closely with security personnel and airport management to ensure that security imperatives and protocols of the ConOps are appropriately aligned. A technology designer should be involved from the project’s inception, including during the ConOps, to help maintain a perspective of practicality.

Geographic location is extremely important. Airports can assess their geographical threat profile using FEMA resources and other guidance to determine threats, vulnerabilities to acts of terrorism, and natural disasters such as flooding, storms, etc. An SOC facility should not be located next to areas that have high threat or vulnerability profiles, such as loading docks, terminals, and concourses or other critical structures. Airports should plan for appropriate non-standard access, and consider the difficulty of gaining access to SOCs inside the airport when the perimeter becomes locked down during emergencies. This includes access for first responders, outside staff, parking, and logistical space for responders.

Airports should plan for logistical support. During emergencies, it is common for staff to occupy the Command and Control Facility for long periods of time, perhaps days. This may require food and supplies and added computer or communications equipment. Planners should ensure there is adequate power; IT bandwidth; space; access for deliveries and people; and, possibly, cooking, sleeping, and bathing facilities.

An SOC facility will require a network operations center with utilities such as power and cooling, including backup provisions. Locating the SOC facility where there is public access within a terminal or other building can have a significant negative impact on survivability, cost, and usability. If possible, airports should locate an SOC where it has the most physical protection from threats. Locating in a basement or ground floor may be subject to flooding, while the highest floor of a building could be affected by storms or high winds. Exterior walls and windows should be avoided because of projectiles or explosions. If an exterior wall or window cannot be avoided, use wall reinforcing techniques or window blast curtains. SOCs should also be protected against attack by a vehicle-borne IEDs; various agencies suggest different setback distances from roadside curbs, depending on building design characteristics. Hardening techniques are addressed in Appendix B.

Having an EOC next to an AOC/SOC can have advantages during emergencies, allowing easier communications among emergency managers and other groups. If possible, a backup SOC should be located in a different area of the airport to protect against utility outages. IT capabilities should enable the airport to manage emergency events even without full SOC functionality.

Architectural elements such as glass walls/doors or movable walls, provide the flexibility to achieve collaboration without disruption. Interior glass walls or doors can also allow visual communications between personnel who staff SOC elements, as well as enable the sharing of video walls. However, glass doors can also present dangerous projectiles if not appropriately isolated from blasts, and for this reason should be built to blast protection standards.

15.5 Basis of Design

The next task is to develop the Basis of Design (BoD) document. The BoD is the formal bridge between the ConOps and the design process, establishing the technical and facility requirements necessary to meet the ConOps goals.

To be clear, the BoD is not a design; it serves as a means for the airport owner-operator and Architectural and Engineering Department to define the parameters of the design by examining optional ways of meeting 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
- Interagency coordination requirements and communications
- Facility location or possible alternatives
- Space requirements and descriptions
- Regulatory and code requirements
- Requirements for redundancy, reliability, and recovery
- Highlevel descriptions of engineered systems (mechanical, electrical, fire protection)
- 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.

15.5.1 Components in the SOC Environment

Consoles and Furniture: Modern SOC facilities utilize computer-based systems with human-machine interaction, connected remotely to the operators' desktops through a network using Keyboard/Video/Mouse control technology. In this environment, true consoles may not be a necessity, and it may be possible to use lighter, less costly, re-configurable furniture where users can move positions by relocating their keyboard, mouse, and screen to a different network connection in another space or even another room.

Large-Format Video Displays Impact Command Center Design: Carefully consider the design of large-format visual displays, which require a cross-disciplinary approach, an understanding of technology and ergonomics, and a traditional architectural and engineering concept. Refer to the Section 12 on CCTV/Surveillance and Section 13 on IT/Communications.

Some critical design aspects include:

- An understanding of how the displays support ConOps, including what will be displayed, who will view it, and who controls it.
- Display Placement: 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 such issues 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.
- Support infrastructure: Each large-format display requires power, cooling, and cabling—elements to address in the design phase. Large-format displays are complex computers that require a similar, high-tech design approach.
- Integration with other systems: Video displays are no longer confined to simply displaying surveillance camera feeds or television broadcasts. Current video displays provide a full spectrum of systems and information sources from anywhere inside or outside the airport. Current control systems for video displays can display a huge range of visual information, including video surveillance cameras, computer screen content, documents, software applications, television, video conferencing, and tracking social media.

- Redundancy in IT Systems: Critical applications and components should have redundant backups that allow for component failure without compromising systems' operation.
  - Server clusters provide for failover to backup servers in milliseconds, with no noticeable delay for users
  - Redundant Array of Independent Disks (RAID) provides increased storage reliability and protection against data loss through redundancy
  - Network switches and routers should utilize redundant components

15.5.2 System Specification and Sourcing

Many airport engineering departments use the Construction Specifications Institute (CSI) MasterSpec specification process. Developing CSI-based designs is an iterative process, with progressively detailed submittals at the 30, 60, 90, and 100 percent milestones for the end user and other appropriate stakeholders to review. Two CSI specification sections, Division 27, Communications, and Division 28, Safety and Security Systems, are especially relevant for the design of an SOC.

SOC design must closely mirror the requirements that evolved from the ConOps into the BoD. However, the design team must be aware of operational and technology changes that may occur during the design development. It must have the capability and flexibility to revisit the BoD to evaluate changes.

15.5.3 Technology

The functions of the SOC are of equal or greater importance than the form, and are heavily dependent on the quality of supporting technology systems. Proper SOC design requires a technology designer to be a key part of the team from the beginning of the process to help the owner make strategic decisions. These early decisions have a significant impact on the success of the project.

The technology design work for an SOC is at least as complex as the architectural/engineering work stream, and the two must progress in parallel. Misalignment of the two is one of the most common causes of cost and schedule overruns, and failure to meet project goals.

15.5.4 Standards

Standards are essential for communication systems and computer networks to function properly. In the United States, the following standards bodies are applicable for airports (see sections on Video Surveillance [Section 12], Communications [Section 13], and Information Security [Section 14] for additional details on applicable standards):

- Institute of Electrical and Electronic Engineers (IEEE): For networking architectures, such as Ethernet networks; for network devices such as a network switch or a wireless access point; and for a variety of electrical power, communications, and other systems
- Telecommunications Industry Association (TIA) for telecommunication facilities and for the cable plants that serve them; ANSI for telecommunication standards with the TIA; NIST for facility, communication, and network security for Federal agencies
- ANSI standards for lighting, acoustics, ergonomics, including visual displays, seating, and other functions
- RTCA DO-230-G *Standards for Airport Security Access Control Systems*: Version G is available at this writing; the document is continually reviewed and updated as often as new technologies and regulations warrant

15.6 Design Guidelines

15.6.1 Space Requirements and Layouts

In considering the optimum layout, users can be arranged with a balance of collaborative face-to-face communication, along with a degree of privacy and acoustic separation in the performance of activities. The ceiling height and beams directly affect how the space will be utilized, the line of sight to shared displays, and how sounds will be perceived. It may be feasible to array consoles in an arc or circle, a cluster, or in a row-by-row schoolroom manner, providing adjacency for related functions. The following spaces typically are provided for airport SOCs:

- Communication and dispatching operations areas
- EOC
- Kitchen, dining area and break room/lounge area with coffee machine, sink, microwave, dishwasher, and related facilities
- Locker rooms
- Supervisor/management offices to include computer access, telephones, radios, fax
- Storage rooms
- Space for bookshelves, file cabinets, printers, and all-purpose print/fax/scan machines
- Conference room
- Server/Network Operation Center

In a public safety dispatch environment, a design that encourages interaction between dispatchers is usually preferred. The face-to-face collaboration between dispatchers during peak periods or major incidents can be an invaluable benefit of collaborative console arrangement.

The overall look and feel of the space should be designed to be soft and subdued, using neutral colors to allow displays to portray skin tones accurately. Lighting should be subdued to reduce eyestrain during prolonged operations. Chairs are critical to users' comfort, and absorptive materials on walls and in ceilings soften the acoustical environment.

15.6.1.1 Console Furniture and Electronic Systems

SOC consoles should permit the call takers and dispatchers 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 as well as CAD map, radio-telephone, access alarm, and CCTV camera LCD monitors in a manner free of distracting interference. Personnel should have the option to stand or sit, and to adjust the lighting and climate on their console. Individual climate control at each console can be provided, to allow for personalization of user ambient light conditions and work space environments. 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.

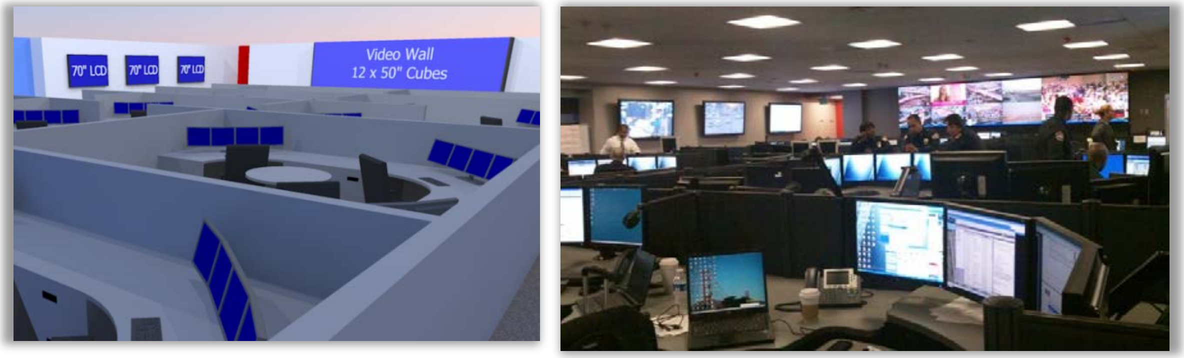
15.6.1.2 Human Factors and Ergonomics

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 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. Techniques such as electronic sound masking and sound deadening materials should be used to avoid aural overload.
- Effective sightlines should be created to provide 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, e.g., 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' work spaces.
- Media relationship issues should be considered and the need for public information release that involves 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 ensure against unauthorized access to sensitive access and 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 on-site 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 make arrangements for overflow personnel to be housed in nearby hotels with shuttles provided.
- Technology should be leveraged to utilize advanced design techniques, such as 3D simulation, when possible. SOC facilities are complex environments that can be difficult to visualize. Using 3D modeling as shown in Figure 15-4 allows airport planners to walk through the design and accurately visualize sightlines and other nuances not visible in a 2D construction drawing.

Figure 15-4. Modeling SOC Areas



Source: System Development Integration, LLC

Electrical infrastructure requires adequate capacity and conditioned back-up power. Space should be allocated for a generator outside the facility, and space for an Uninterruptible Power Supply (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 non-existent.

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, including possible satellite connectivity as a backup.

Envelope electromagnetic/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 facility, wireless repeaters may be necessary when the building’s structure blocks signals. Planners should design for multiband repeaters that will work with all the wireless devices being used.

Resupply and storage space for essential supplies, such as food, fuel for a generator, batteries, and office supplies, should be considered in the design. Satellite dishes will require space on the roof and line-of-sight access to satellites. They will also need periodic maintenance; roof layouts and access should be planned accordingly.

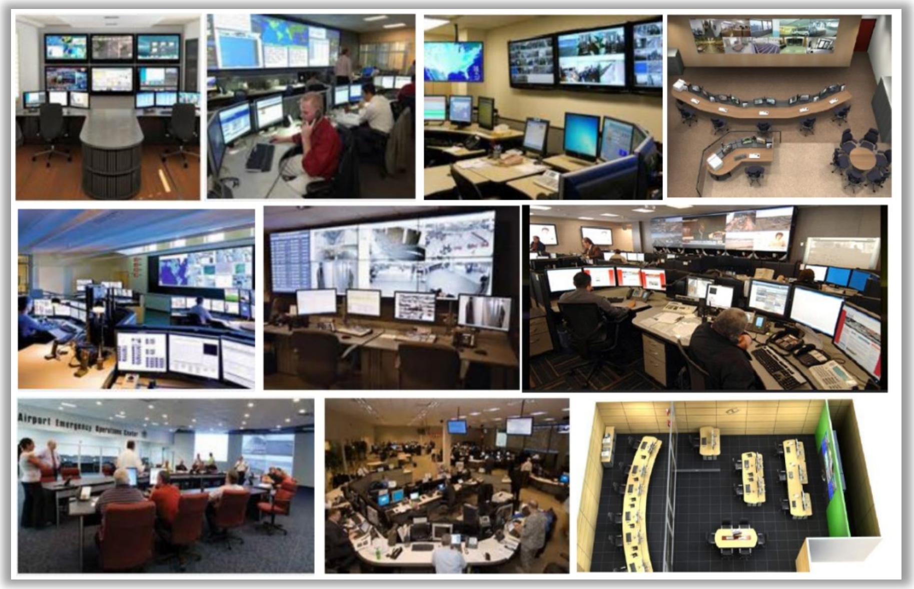
Critical applications and components should have redundant backups that allow for component failure without compromising system operations. Server clusters provide for failover to backup servers in milliseconds, with no noticeable delay for users. RAID provides increased storage reliability and protection against data loss through redundancy. Network switches and routers should utilize redundant components. Data backups should be performed periodically, and offsite backups should be considered as a safeguard against complete facility compromise.

The design process must consider not only the logical transmission, reception, and presentation of data from literally hundreds of simultaneous voice/data/video reporting points, but also a requirements assessment to determine the necessary balance between automated and human interfaces (e.g., how the information will flow to and from the SOC and other SOC elements).

15.6.2 Displaying Information for Operations

SOC, AOC, and EOC configurations vary widely, depending on the scale of airport operations, operator preferences, functions to be performed, budgets, and other factors, as Figure 15-5 below illustrates:

Figure 15-5. Typical Airport SOC-AOC-EOC Configurations



Source: TranSecure, Inc.

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 (2 vertical x 3 horizontal), and can expand to many times these numbers subject to wall area, power and cooling, aesthetics, and budgetary constraints.

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.

15.6.3 Other Design Issues

15.6.3.1 Americans with Disabilities Act

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 Americans with Disabilities Act 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.

15.6.3.2 Internet

Broadband internet access is vital for SOC participants, especially during emergencies, for communicating with external agencies when traditional wire or radio links are unavailable. Internet access will be essential for participants in the EOC, who in many instances will be representing other agencies in remote locations and will need access to their home networks.

15.6.3.3 News/Weather Feeds

Satellite and cable television feeds should be provided to allow 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.

15.6.3.4 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.

15.6.4 Electrical Power

Under all conditions, sufficient input power feeds must be provided to support the entire electrical loads of the SOC for the operation of the communications network and its related support systems and equipment. Normal power should include at least one circuit from a utility distribution system and a second from an emergency generator, with automatic transfer upon loss of power.

In addition, all critical equipment in the SOC, its supporting elements, and in Server/Network Operations Centers should be provided with UPS backed up by the emergency generators to sustain operations in the event of extended failure of conventional power. IT backup policies vary by facility. The UPS period of operation specified for IT-connected devices may be as little as 30 minutes—in which case, for a 24-hour emergency operation, they should also be connected to any generators/standby power units used for the SOC.

15.6.5 Mapping

The mapping module has the capability of displaying multilevel maps and corresponding alarms (e.g., fire alarm, intruder alert, intercom activation, etc.) through the event 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.

15.6.6 Computer-Aided Dispatch

When an SOC is primarily an airport police or security operation, such as a PSAP, 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 VCIN, NCIC, E911, voice radio, mapping, CCTV video camera and digital video recording system, access control systems, and entry and fire alarm systems.

Computer-Aided Dispatch workstation operational modes should include:

- Call taker
- Police Dispatcher
- Fire Dispatcher
- Supervisor
- Fire Supervisor
- Police Station
- Fire Station
- System Manager

All workstations should have the following capabilities:

- User logon or logoff
- Send/receive administrative messages
- Retrieve event status – past and current
- Access dynamic mapping information

- Address validation
- Self- or field-initiated activities
- Create incident report for any events
- Paging
- Add information to an event history

15.6.7 Communications Infrastructure

SOC communications integrated with other subsystems should ensure that operators are provided with sufficient actionable information on alert and alarm events to be able to analyze, react, and/or dispatch appropriately. SOC communications systems should be network-based to ensure data integrity, full connectivity among all system components, and appropriate system monitoring and diagnostics. It should also be sufficiently scalable to allow expansion.

A number of technology issues are relevant to implementing the communication network, such as bandwidth analysis, communications security, network topology, communication redundancy, transmission modes or protocols, reserve capacity, and transmission media.

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.

The network should be sized to have enough excess operating capacity to maintain the initial operating traffic parameters (to be determined), and accommodate sustained peak loads during download/upload of information without impact on operational response times. In addition, there must be reserved capacity for traffic reroutes during the failure of an interconnecting node within the network.

Priority-reserved capacity (outside of the excess capacity for peak operations) is required for emergencies to allow multiple locations to be accessed from a central command center to coordinate database lookup and updates. When services for emergencies are provided by common carriers, such as telephone service, previous arrangements should be made.

Access to a wide area network by a commercial telecommunications and network service provider should include both guaranteed minimum bandwidth and guaranteed surge bandwidth, the latter to handle incident management. The guarantees of bandwidth should be set forth in a written service level agreement with the service provider.

Under FCC rules, certain unlicensed devices are exempt from regulation, and may be freely used so long as they conform to technical standards established by the FCC. For wireless LANs operating in the Wi-Fi bands of 3 GHz and 5 GHz, peak power and radiated signal strength limits have been established that limit wireless coverage.

In addition to commercial cellular and wireless LAN services, other types of commercial services widely used for everyday non-critical communications generally fall into one of the following categories.

- Specialized Mobile Radio (SMR) may provide mobile dispatch and data communications services. Users of SMR systems can communicate between single radios or simultaneously to a group of users. Interoperability outside of the service may be limited due to the lack of common standards and protocols, which is further compounded by the fact that SMR systems are licensed across three different frequency bands (220 MHz, 800 MHz and 900 MHz).
- Mobile Satellite Service offers digital broadcast capability, which allows the dispatcher to speak to a single user, a group of users, or all network users. Users can in turn communicate with members in predefined talk groups. Users within a talk group can communicate via a one-way group call or through standard two-way communication.
- Voice-over-IP voice and collaborative services are offered by providers such as Skype and implemented over wired networks, wireless LANs, and cellular services. Skype communications are secured.
- Trunked radio systems, typically operating in the 800 MHz band, provide all dispatchers and field units with the capability to verbally communicate with various mutual aid channels to support regional interoperability.

15.6.7.1 System Testing and Verification

SOC testing activities may take a variety of forms and include system test plan development, system test procedure development, System Qualification Testing and/or Factory Acceptance Testing, Site Installation Testing, and Operational Testing.

Designers should ensure that the new SOC meets specified operational and functional capabilities, and verify that the SOC is ready to be handed over to and operated by the user.

15.6.8 Cybersecurity

Because of the computer-based architecture of security systems and the interconnected nature of the web-based world, it is imperative that all systems are secured against cyber threats. This topic is covered in Section 14 of this document. Command and Control Facility designers must create a plan for cybersecurity that addresses design challenges like firewalls, virus detection, intrusion detection, and identity management.

15.6.9 Future Proofing and Adapting to New Technologies

Finally, the development of a new SOC does not typically happen in isolation. The new facility may be developed over a multi-year period, often within a new or existing facility upgrade, during which it must integrate with existing or upgraded infrastructure. Where practical, consideration should be given to alignment with growing national guidance and standards for information sharing and Command and Control Center design. Coordination with other airport projects to avoid conflicts or unnecessary duplication of effort is essential. This can avoid issues such as inadequate power, conflicts for contractor access or logistical spaces, or integration issues with the network or other airport technology systems.

Beyond the issue of coordination with existing projects, future projects, and changing requirements, designers should understand that technology will clearly continue to change over time. This often results in evolutionary change for SOC operations as new technologies become available. Understanding technology trends, and including flexibility into design parameters where possible, will allow for easier future adaptation.

15.6.9.1 Wearables and Internet of Things

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.

Data from wearable sensors will only increase as those items become more commonplace. SOCs 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.

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.

15.6.9.2 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. FEMA has now fully embraced social media by maintaining numerous social media accounts and developing training for social media management and use. Similarly, organizations such as the International Association of Chiefs of Police have established programs to promote social media use by law enforcement.

Integration of social media into SOCs 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 SOCs of the future would do well to anticipate social media use in their SOC designs.

15.7 Trends

Technology trends such as mobile technology, 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. SOCs 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 mobility and 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 sensor 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, or the integration of audio or motion sensors, or social media monitoring systems that provide alerts or alarms.

In addition to the more tactical and operational use of analytic tools, big data analysis may also help with strategic decision making. The large data fields, particularly from video surveillance systems, lend themselves to big data analysis and other operational efficiencies. In particular, analysis offers:

- Increased integration of access control, video surveillance, perimeter intrusion detection, and other security system functions with geolocation and CADD drawings to enhance incident analysis and response by SOC operators.
- Increased integration and/or colocation of SOC, AOC, EOC, and Police Dispatch functions because of shared incident responsibilities and IT network facilities and equipment, including wireless capabilities for mobile response units.
- Increased intermingling of formerly discreet data sources and expanded availability of data to support decision making and forensic analysis.
- Major manufacturers are exploring applications where virtual reality can immerse a command center supervisor in an incident scene. By using a combination of virtual reality and eye-interaction technologies to navigate through video and data feeds, incident responses can be quickly coordinated and information shared widely to help guide officers at the scene.

15.8 Checklist

Security Operations Centers Checklist

□ Develop operational requirements using the ConOps process
  - ID SOC functions/requirements
  - ID standards to be adopted
  - ID legacy systems to retain
  - ID public access and media needs
  - ID social media use in SOC
  - ID interoperability requirements
  - Involve IT staff in discussions

□ SOC Planning and Design
  - Establish relation to EOC, AOC
  - ID limits –space, staff, budget
  - Model SOC at Basis of Design
  - 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, event management
  - Video wall size, configuration
  - Smart phone accommodations
  - Observer access, isolation

Detailed design information for the SOC applications, networking, communications, CCTV and supplementary functionality can be found in complementary sections throughout this document, as well as in industry and government guidance documents noted in the bibliography.

REFERENCES

Note

DHS, FAA, TSA, and other sources/agencies listed below periodically update many of the documents, rules, regulations, statutes, and codes referenced in this bibliography. These updates sometimes change the entire document, but more often the changes are only in segments as new information becomes available. The reader should seek guidance directly from the source to ensure the referenced document is the most current version.

Advisory Circulars

The latest issuance of the following advisory circulars may be obtained from the Department of Transportation, Utilization and Storage Section, M-443.2, Washington, D.C. 20590. Also see the FAA website at http://www.faa.gov/regulations_policies/advisory_circulars/ for an index of all circulars; the series of advisory circulars (AC) designated "150" applies to airports. Additional contact names and numbers may also be found there.

1. 00-2, Advisory Circular Checklist—Contains a listing of all current ACs.
2. 129-3, Foreign Air Carrier Security. Provides information and guidance on the implementation of sections 129.25, 129.26, and 129.27 of FAR § 129. Note: the security aspects of the FAR § 129 regulation have been superseded by 49 CFR § 1546, but the AC still exists for operational guidance for foreign air carriers only.
3. 150/5200-31C (June 19, 2009) Airport Emergency Plan (Consolidated AC includes Change 2)
4. 150/5300-13, Airport Design
5. 150/5360-13, *Planning and Design Guidelines for Airport Terminal Facilities*. Furnishes guidance material for the planning and design of airport terminal buildings and related facilities.
6. 150/5370-10, Standards for Specifying Construction of Airports

Note: As this Guidelines document is being finalized, FAA has released a *draft* for industry comment reflecting many changes in AC 150/5360-13A, *Planning and Design for Airport Terminal Facilities*. When published, AC 150/5360-13A will cancel both AC 150/5360-13 and AC 150/5360-9, *Planning and Design Guidelines for Airport Terminal Facilities at Non-Hub Locations*.

Government Reports and Regulations

Government reports may be obtained from the National Technical Information Services (NTIS), 5301 Shawnee Road, Alexandria, VA 22312; Tel: (703) 605-6040 (http://www.ntis.gov/).

Most reports may also be obtained directly from the originating government agency and are often also available on the agency's website.

Aviation and Transportation Security Act (ATSA). Public Law 107-71 49 CFR SubChapter C: Civil Aviation Security [all]49 CFR § 1520 Protection of Sensitive Security Information

49 CFR § 1540 Civil Aviation Security General Requirements.

49 CFR § 1542 Airport Security.

49 CFR § 1544 Aircraft Operator Security.

49 CFR § 1546 Foreign Air Carrier Security.

49 CFR § 1548 Indirect Air Carrier Security.

14 CFR § 139 Certification and Operations: Land Airports

14 CFR § 139.325—Airport emergency plan.

Homeland Security Act, Public Law 107-296

Planning Guidelines and Design Standards (PGDS) Ver. 5.0 for Checked Baggage Inspection Systems (CBIS), TSA. The PGDS is updated annually and can be accessed at: PGDS for CBIS.

Electronic Baggage Screening Program (EBSP). Guidance and sample documentation will continue to be reviewed, updated and posted to: EBSP TSA.

National Incident Management System, December 2008, United States Department of Homeland Security, NIMS 2008.

TSA NEDCTP Canine Training & Evaluations Branch, TSA K-9 Contact Information National Explosives Detection Canine Team Program.

Chemical & Biological Agent Resources and guidance may be obtained from TSA, FEMA, FBI, Department of Energy (DOE), CDC.

Airport Planning, Security, and Transportation and Facility Security Reports

(Where publication dates are not shown, the publication or document is typically updated regularly, or annually, and should be reviewed in its most recent edition. Some publications are free and others available for purchase.)

1. Airport Planning Manual—Master Planning, Part 1 (Doc 9184). International Civil Aviation Organization.
   www.icao.int (available for purchase)
2. Transit Security Design Considerations, Final Report, John A. Volpe National Transportation Systems Center, U.S. Department of Transportation, November 2004.
   https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/ftasesc.pdf (accessed July 2, 2016)
3. *DoD Minimum Antiterrorism Standards for Buildings 2012*, U.S. Department of Defense, October 2003 (including change 1, 19 January 2007) and the National Institute of Building Sciences (http://www.wbdg.org/) Physical Security. U.S. Army FM 3.19.30, January 2001.
4. Existing and Potential Standoff Explosives Detection Techniques, 2004, Board of Chemical Sciences and Technologies, The National Academies Press, 2004. Available for purchase at: Existing and Potential Standoff Explosives Detection Techniques | The National Academies Press
6. *Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism*, Edwards, Dr. Donna M., et al, Sandia Berkley National Laboratory, Albuquerque, New Mexico 87185 and Livermore, California 94550. SAND2005-3237/LBNL-54973 (II), May 2005, prepared for the U.S. Department of Energy.

7. Glazing Hazard Mitigation, by Joseph L. Smith, PSP and Nancy A. Renfroe, PSP, Applied Research Associates, Inc., http://www.wbdg.org/resources/glazingmitigation.php
8. Building Security: Handbook for Architectural Planning and Design, Barbara A. Nadel, published by McGraw-Hill Professional, April 2004. Available for purchase from Internet book sites.
9. *International Standards and Recommended Practices—Security—Aerodromes*—Annex 14 to the Convention on International Civil Aviation. Volume I, Aerodrome Design and Operations. International Civil Aviation Organization. Available for purchase from: http://www.icao.int/
10. International Civil Aviation Organization—*Standards and Recommended Practices—Security—Safeguarding International Civil Aviation Against Acts of Unlawful Interference*—Annex 17 to the Convention on International Civil Aviation. Available for purchase: http://www.icao.int/
11. International Civil Aviation Organization—*Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference* (Doc 8973, restricted distribution). International Civil Aviation Organization. Available for purchase http://www.icao.int/
12. National Fire Codes NFPA 101—Life Safety Code. National Fire Prevention Association. Available for purchase from www.nfpa.org
13. National Fire Codes NFPA 415—*Standard on Construction and Protection of Airport Terminal Buildings, Fueling Ramp Drainage, and Loading Walkways*, 2008 Edition, National Fire Prevention Association. Available for purchase from: http://www.nfpa.org
14. *Merritt Risk Management Manual*, available for purchase from Silver Lake Publishing at: http://www.silverlakepub.com/Merritt_Risk_Management_Manual.php
15. RTCA/DO-230G, *Standards for Airport Security Access Control Systems* RTCA/DO-230G Publications are available for purchase. DO-230H scheduled for release early 2017H scheduled for release early 2017.
16. RTCA/DO-221, *Guidance and Recommended Requirements for Airport Surface Movement Sensors* (1994), RTCA/DO-221 Available for purchase.
17. *Security Guidelines for General Aviation Airports*. Aviation Security Advisory Committee. (2004) http://www.ct.gov/demhs/lib/demhs/airport.pdf
18. Terrorism in the United States—Terrorist Research and Analytical Center. Counter Terrorism Section, Criminal Investigative Division. Federal Bureau of Investigation. Annual.
19. Vulnerability Identification Self-Assessment Tools (Hazmat Risk Assessment and Vulnerability Evaluation; Port and Intermodal Vulnerability Identification Self-Assessment; and Mass Transit Vulnerability Identification Self-Assessment), Transportation Security Administration, U.S. Department of Homeland Security https://www.dhs.gov/xlibrary/assets/pso_cat_tsa.pdf
20. DOE Vulnerability and Risk-Assessment Methodology, Vulnerability and Risk Management Program, U.S. Department of Energy, 2001 (Available through the Electricity Sector—Information Sharing and Analysis Center (ESISAC) http://www.esisac.com/
21. Lessons Learned from Industry Vulnerability Assessments and September 11th, a presentation of Argonne National Laboratory, U.S. Department of Energy, December 2001
22. *The Public Transportation System Security and Emergency Preparedness Planning Guide*, DOT-FTA-MA-26-5019-03-01, Federal Transit Administration, U.S. Dept. of Transportation, January 2003 https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/PlanningGuide.pdf

23. *A How-To Guide Mitigate Potential Terrorist Attacks Against Buildings*, FEMA 452, January 2005, Federal Emergency Management Agency, U.S. Department of Homeland Security http://www.fema.gov/library/viewRecord.do?id=1938 (Available for download, free)
24. Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks, FEMA 427, December 2003, Federal Emergency Management Agency https://www.fema.gov/media-library-data/20130726-1455-20490-6114/fema427.pdf
25. Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, FEMA 426, December 2003, Federal Emergency Management Agency, U.S. Department of Homeland Security http://www.fema.gov/library/viewRecord.do?id=1559
26. The Design and Evaluation of Physical Protection Systems, Mary Lynn Garcia, published by Butterworth-Heinemann, 2001. Available for purchase at Internet book sites.
27. *Progressive Collapse Analysis and Design Guidelines for New Federal Office Buildings and Major Modernization Projects*, (U.S. General Services Administration, June 2003) http://cement.org/buildings/US-GSA-ProgCollapse-SEI-04.pdf GSA and 08-Security Design http://www.gsa.gov/portal/category/21057
28. Chain Link Fence Manufacturers Institute Security Fencing Recommendations, Chain Link Fence Manufacturers Institute, http://www.chainlinkinfo.org/wp-content/uploads/2015/08/CLFMI-SECURITY-FENCING-RECOMMENDATION-20141.pdf
29. *TSA Checkpoint Design Guide* (CDG) Revision 6.1, June 01, 2016
30. *TSA Security Checkpoint Layout Design Reconfiguration Guide* (2006) http://www.aci-na.org/static/entransit/Checkpoint_Layout_Design_Guide_v1r0-0.pdf
31. American Water Works Association, AWWA J100-10 (R13) Risk and Resilience Management of Water and Wastewater Systems (RAMCAP). Google Preview. ISBN: 9781583217887. Publisher: [PDF]RAMCAP Basics – ORWARN www.orwarn.org/files/Morley-RAMCAP%20Basics.pdf
32. Russell Lundberg and Henry Willis, "Assessing Homeland Security Risks: A Comparative Risk Assessment of 10 Hazards," Homeland Security Affairs 11, Article 10 (December 2015); and Russell Lundberg and Henry Willis, "Deliberative Risk Ranking to Inform Homeland Security Strategic Planning," Journal of Homeland Security and Emergency Management 13, no. 1 (April 2016) (DOI: 10.1515/jhsem-2015-0065)

Federal Inspection Service (FIS) Area Applicable Laws and Regulations

(In effect at the time of publication)

To ensure that all international passengers and their baggage arriving in the United States are properly inspected to determine their admissibility to the United States, U.S. Customs and Border Protection (CBP), in conjunction with the U.S. Fish and Wildlife Service (FWS) and the Public Health Service (PHS), maintains oversight of the Federal Inspection Service (FIS) area at airport passenger processing facilities.

1. Section 233(b) of the Immigration and Nationality Act (INA) https://www.gpo.gov/fdsys/pkg/BILLS-114s1593is/html/BILLS-114s1593is.htm Section 233(b) of the INA requires the transportation line or their agent, the Airport Operator, to "provide and maintain at its expense suitable landing stations, approved by the Attorney General."
2. Title 8 part 234, section 4 of the CFR: International Airports for Entry of Aliens.

http://www.uscis.gov/ilink/docView/SLB/HTML/SLB/0-0-0-1/0-0-0-11261/0-0-0-22435/0-0-0-22459.html#0-0-0-14953

3. Presidential Decision Directives. www.fas.org/irp/offdocs/nspd/index.html

   The Presidential Decision Directive (PDD) series is used to promulgate Presidential decisions on national security matters.

4. HSPD -12- Addresses IT services. Implementing this directive is expected to involve personal identification authentication using biometrics and is likely to be reflected in TSA enhancements for access control at airports during the life of this document. http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

5. CBP *Airport Technical Design Standards—Facility Standards for Passenger Processing Facilities at Airports and Pre-Clearance Sites, Customs and Border Protection*, U.S. Department of Homeland Security.

6. Frequently Asked Questions (FAQs) About CBP Technical Standards for Air Passenger Processing at U.S. Ports of Entry, Customs and Border Protection, U.S. Department of Homeland Security, March 2004 http://www.cbp.gov/

Miscellaneous Regulations, Reports, and Resources

1. Circular 150/5360-12E (http://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/74209), updated June 2010 recommends the use of these Guidelines for designing airport terminal signing systems

2. U.S. Department of Justice Americans with Disabilities Act (ADA) for regulatory requirements and guidance. http://www.ada.gov/2010ADAstandards_index.htm

3. Ergonomic and workplace standards and requirements of the U.S. Department of Labor Occupational Safety & Health Administration (OSHA) are available at the following websites: www.osha.gov/SLTC/ergonomics www.osha.gov/SLTC/etools/baggagehandling/index.html http://www.osha.gov/SLTC/etools/computerworkstations/components_monitors.html

4. ASTM F2656—07 *Standard Test Method for Vehicle Crash Testing of Perimeter Barriers*, American Society for Testing and Materials (ASTM), http://www.astm.org/Standards/F2656.htm

5. IEEE802, IEEE 802 LAN/MAN Standards Committee, http://www.ieee802.org/

6. Personal Identity Verification (PIV) of Federal workers and contractors, http://csrc.nist.gov/groups/SNS/piv/index.html http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf http://csrc.nist.gov/publications/nistpubs/800-79-1/SP800-79-1.pdf

7. International Building Code Council

8. Building Industry Consulting Service International, Inc. (BICSI), https://www.bicsi.org/default.aspx

9. National Electric Code (NEC), http://www.neccodebooks.com/

10. Telecommunications Industry Association (TIA), http://www.tiaonline.org/

11. “Administrative Standard for Telecommunications Infrastructure,” TIA/EIA-606A, http://az776130.vo.msecnd.net/media/docs/default-source/contractors-and-bidders-library/standards-guidelines/it-standards/tia-606-b.pdf?sfvrsn=2

12. Electronic Industry Alliance (EIA). EIA ceased operations in Dec 2010. EIA Standards are managed by ECA, http://ec-central.org/index.cfm

13. American National Standards Institute (ANSI) ANSI/IESNA RP-104, ANSI Standards Store https://www.ansi.org/

14. NIST Risk Management Framework (RMF), http://csrc.nist.gov/groups/SMA/fisma/framework.html

15. NIST 800-53 “controls,” http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

16. American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), http://www.ashrae.org

17. National Emergency Number Association, NENA Master Glossary of 9-1-1 Terminology, http://www.nena.org

18. IATA, The Airport Development Reference Manual (ADRM)

19. National Safe Skies Alliance

20. Common Use Passenger Processing Systems (CUPPS)

21. Institute of Electrical and Electronic Engineers (IEEE)

22. Internet Engineering Task Force (IETF)

23. International Telecommunications Union (ITU)

24. The International Organization for Standardization (ISO)

25. Federal Communication Commission (FCC)

26. The Critical Infrastructure Key Resource (CIKR) Annex

27. National Transportation Safety Board

28. Homeland Security Affairs, Assessing Homeland Security Risks: A Comparative Risk Assessment of 10 Hazards

29. Lundberg, Russell, Comparing Homeland Security Risks Using a Deliberative Risk Ranking Methodology

30. The National Academies Press, Privacy Research and Best Practices: Summary of a Workshop for the Intelligence Community (2016) PDF downloadable https://www.nap.edu/catalog/21879/privacy-research-and-best-practices-summary-of-a-workshop-for?utm_source=NAP+Newsletter&utm_campaign=77d1f58b71-NAP_mail_new_2016_03_03&utm_medium=email&utm_term=0_96101de015-77d1f58b71-103232121&goal=0_96101de015-77d1f58b71-103232121&mc_cid=77d1f58b71&mc_eid=6b09cd3bb4

31. Souppaya, Murugiah and Karen Scarfone, National Institute of Standards and Technology. *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

32. Cybersecurity Curriculum Resources https://niccs.us-cert.gov/education/curriculum-resources

33. Jayavardhana Gubbia, Rajkumar Buyyab, Slaven Marusic, Marimuthu Palaniswami, Department of Electrical and Electronic Engineering, The University of Melbourne, Vic - 3010, Australia and the Department of Computing and Information Systems, The University of Melbourne, Vic - 3010,

Australia, *Future Generation Computer Systems* journal homepage www.elsevier.com/locate/fgcs "Internet of Things (IoT): A vision, architectural elements, and future directions"

34. Unified Facilities Criteria (UFC), Emergency Operations Center Planning and Design
35. Chaffey, Dave, "Global social media research summary," (October 13, 2015), a compilation of social media statistics of consumer adoption and usage http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/
36. MASTERSPEC
37. Garfinkel, Simson, L. "De-Identification of Personal Information." NISTIR 8053. National Institute of Standards and Technology, Information Access Division, Information Technology Laboratory, October 2015. This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.IR.8053
38. Etue, David, VP, Corporate Development Strategy, "Social Media: Leveraging Value While Mitigating Risk." Safeguarding Health Information: Building Assurance through HIPAA Security NIST/HHS OCR 2013 (PPT) (May 21, 2013)
39. Secured Cities, May the Social Media Force Be With You, Mar 23, 2015
40. Bauer, Harald, Mark Parel and Jan Viera, "The Internet of Things: Sizing up the opportunity"
41. The Department of Homeland Security, The Department of Justice, *Privacy and Civil Liberties Interim Guidelines: Cybersecurity Information Sharing Act of 2015*, February 16, 2016
42. CIO Council, *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*, Information Security and Identity Management Committee (ISIMC), Network and Infrastructure Security Subcommittee (NISSC), Web 2.0 Security Working Group (W20SWG) Version 1.0, September 2009, www.energy.gov/sites/prod/files/maprod/documents/SecureSocialMedia.pdf

Additional References for Section 12, Video Surveillance, Detection and Distribution Systems

1. *Defining Video Quality Requirements: A Guide for Public Safety*, Version 1.0, developed by the Video Quality in Public Safety Group under sponsorship of the U.S. Department of Homeland Security Office of Interoperability and Compatibility (OIC), and the U.S. Department of Commerce Public Safety Communications Research (PSCR) program, Washington D.C. (2010) http://www.safecomprogram.gov/NR/rdonlyres/5BCA1CBF-1500-4B29-9370-81B823575DE8/0/3aVideoUserRequirementGuidedoc.pdf
2. "The Target Task Performance (TTP) Metric: A New Model for Predicting Target Acquisition Performance," Technical Report AMSEWL-NV-TR-230, U.S. Army CERDEC, Ft. Belvoir VA (2004) http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA422493&Location=U2&doc=GetTRDoc.pdf
3. "New Metric for Predicting Target Acquisition Performance," R. Vollmerhausen et al, Optical Engineering (43)11, pp. 2806-2818 (2004) http://opticalengineering.spiedigitallibrary.org/article.aspx?articleid=1100666
4. "RFC 2326: The Real Time Streaming Protocol (RTSP)," the Internet Engineering Task Force (IETF) (1998) http://www.ietf.org/rfc/rfc2326.txt
5. "Electro-Optical System Design, Analysis, and Testing," M. Dudzik, Ed., in "The Infrared and Electro-Optical System Handbook, Vol. 4," Environment Research Institute of Michigan, Ann Arbor MI (1993)

http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA364024&Location=U2&doc=GetTRDoc.pdf

6. "Modeling target acquisition tasks associated with security and surveillance"; Vollmerhausen and Robinson, Applied Optics, Vol. 46, Issue 20, pp. 4209-4221 (2007) http://www.opticsinfobase.org/abstract.cfm?uri=ao-46-20-4209

7. Representative manufacturer web sites which contain tutorials and white papers on networking video surveillance, on performance metrics including Pixel per Foot (PPF), and related subjects:

- Axis Communications: https://www.axis.com/dk/en/products/network-cameras
- Bosch Security Systems: http://stna.resource.bosch.com/documents/WhitePaper_enUS_2233713163.pdf
- Cisco Systems: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVS-DesignGuide/IPVSchap4.html
- Cohu Costar: http://cohuhd.com/Files/white_papers/CohuHD_HD_Resolution_Solutions.pdf
- Theia Technologies: http://www.sdmmag.com/SDM/Home/Files/PDFs/ResolutionCalculation_whitepaper.pdf

National Safe Skies Alliance and NAS-TRB Support Programs

Although the FAA does not have airport specific cybersecurity research projects, the FAA Office of Airports sponsors two industry-driven applied research programs:

- The National Safety Skies Alliance (Safe Skies), http://www.sskies.org, Program for Applied Research in Airport Security (PARAS), an industry-driven applied research program for near-term practical solutions to security challenges facing the airport operators. It is funded by the FAA AIP funds and managed by Safe Skies. The PARAS program annually issues research project solicitations. Safe Skies' PARAS Manager is Jessica Grizzle, jessica.grizzle@sskies.org.
- The ACRP is an industry-driven applied research program, also funded by the FAA AIP. The program is managed by the Transportation Research Board (TRB) of the National Academies of Sciences (NAS), Engineering, and Medicine, http://www.trb.org/ACRP/ACRP.aspx.

  Upcoming CRP Projects are listed at the TRB ACRP website, http://www.trb.org/NCHRP/UpcomingCRPProjects.aspx. The TRB ACRP Manager is Michael Salamone, msalamone@nas.edu.

These two industry-driven FAA-funded airport research programs address many airport-related security issues, such as Command and Control and cybersecurity. Examples for airport security planning, design, and construction include:

- Research projects initiated by Safe Skies in 2015 under the PARAS program:

  PARAS 0001 – Guidebook for Criminal History Records Checks (CHRCs) and Vetting Aviation Workers

  PARAS 0002 - Companion Guide to U.S. Customs and Border Protection's *Airport Technical Design Standards*

  PARAS 0003 - Enhancing Communication and Collaboration Among Airport Stakeholders

PARAS 0004 – Update TSA’s Recommended Security Guidelines for Airport Planning, Design, and Construction Document (*under which these Guidelines are being developed*)

PARAS 0005 - Airport Breach Classification and Best Practices

PARAS 0006 - Employee Inspection Synthesis

- Recent publications and upcoming research projects under the TRB ACRP program:

  ACRP Report 144, Unmanned Aircraft Systems (UAS) at Airports: A Primer, published September 30, 2015

  ACRP Report 143, Guidebook for Air Cargo Facility Planning and Development, published October 2, 2015

  ACRP Report 140, Guidebook on Best Practices for Airport Cybersecurity, published July 9, 2015

  ACRP Report 131, A Guidebook for Safety Risk Management for Airports, published May 23, 2015

  ACRP Report 128, Alternative IT Delivery Methods and Best Practices for Small Airports, published March 2, 2015

- Upcoming projects:

  ACRP 01-29, State Aviation Data Collection and Analysis

  ACRP 01-32, Update Guidebook for Managing Small Airports

  ACRP 01-33, Preparing for the Connected Airport and the Internet of Things

  ACRP 02-69, Integrating Airport Sustainability Plans with Environmental Analyses

  ACRP 02-72, Developing a Renewable Resource Strategy at Airports

  ACRP 04-20, Airport Emergency Operations Centers Design Guide

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND DEFINITIONS OF TERMS

A/C Advisory Circular (FAA)

ACAMS Access Control and Alarm Monitoring System

Access Control A system, method or procedure to limit and control access to areas of the airport. 49 CFR § 1542 requires certain airports to provide for such a system.

ADA Americans with Disabilities Act

AEP Airport Emergency Plan

AIP Airport Improvement Program by the FAA. The program's broad objective is to assist in the development of a nationwide system of public-use airports adequate to meet the current projected growth of civil aviation. It provides funding for airport planning and development projects at airports included in the National Plan of Integrated Airport Systems (NPIAS).

Air Carrier An entity or person who undertakes directly by lease, or other arrangement, to engage in air transportation. Also known as Aircraft Operator. This includes an individual, firm, partnership, corporation, company, association, joint-stock association, governmental entity, trustee, or similar representative of such entities.

Air Carrier Aircraft An aircraft that is being operated by an air carrier and is categorized, as determined by the aircraft type certificate, as either a large air carrier aircraft if designed for at least 31 passenger seats, or a small air carrier aircraft if designed for more than 9 passenger seats but less than 31 passenger seats.

Aircraft Loading Bridge An above-ground device through which passengers move between an airport terminal and an aircraft. (Often referred to by the brand name Jetway)

Aircraft Operator A person who uses, causes to be used, or authorizes to be used an aircraft, with or without the right of legal control (as owner, lessee, or otherwise), for the purpose of air navigation including the piloting of aircraft, or on any part of the surface of an airport.

Aircraft Stand A designated area on an airport ramp intended to be used for parking an aircraft.

Airline An air transportation system including its equipment, routes, operating personnel, and management.

Airport An area of land or other hard surface, excluding water, that is used or intended to be used for the landing and takeoff of aircraft, including any buildings and facilities.

Airport Operating Certificate A certificate, issued under FAR § 139, for operation of a Class I, II, III, or IV airport.

Airport Operator A person that operates an airport serving an aircraft operator or a foreign air carrier required to have a security program under 49 CFR § 1544 or 49 CFR § 1546.

Airport Ramp Any outdoor area, including aprons and hardstands, on which aircraft may be positioned, stored, serviced, or maintained.

Airport Security Committee A TSA-encouraged airport security committee made up of persons and organizations having a direct interest in the security decisions being made and their impact on the airport security environment. Participants might include airlines, concessions, other tenants, FBOs, and TSA representatives, among others. An Airport Security Committee is an advisory panel and a broad-based resource for airport security matters; it is not empowered to issue directives.

Airport Security Program An airport-specific security program approved by TSA under 49 CFR § 1542.101.

Airport Tenant Any person, other than an aircraft operator or foreign air carrier with a security program under 49 CFR § 1544 or 49 CFR § 1546 that has an agreement with the airport operator to conduct business on airport property.

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

Airside Those sections of an airport beyond the security screening stations and restricting perimeters (fencing, walls or other boundaries) that includes runways, taxiways, aprons, aircraft parking and staging areas, and most facilities that service and maintain aircraft.

Alarm Resolution To resolve an alarm during any part of the checked baggage screening process and determine whether an individual’s property contains prohibited items

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

AOSSP Aircraft Operator Standards Security Program (AOSSP or SSP), the detailed, nonpublic document an aircraft operator regulated under 49 CFR § 1544.

Approved Unless used with reference to another person, means approved by TSA.

Apron A defined area, on a land aerodrome, intended to accommodate aircraft for purposes of loading or unloading passengers, mail or cargo, fueling, parking or maintenance. Often called a ramp.

ARFF Aircraft Rescue and Fire Fighting—A term used to identify the facility, operation or personnel engaged such activities.

ASC Airport Security Coordinator—An individual designated by an airport operator to serve as the primary contact with TSA for security-related activities and communications.

ASP Airport Security Program under 49 CFR § 1542.101.

ASTM American Society for Testing and Materials

ATC Air Traffic Control

ATCT Airport Traffic Control Tower

ATO Airport Ticket Office—A place at which the aircraft operator sells tickets, accepts checked baggage, and through the application of manual or automated criteria, identifies persons who may require additional security scrutiny. Such facilities may be located in an airport terminal or other location, e.g., curbside at the airport.

ATSA Aviation and Transportation Security Act of 2001

ATSP Airport Tenant Security Program

AVSEC Aviation Security

AVSEC Measures Aviation Security Contingency Measures (contained in the ASP)

Baggage Claim Area Space normally located in the passenger terminal building, where passengers reclaim checked baggage.

Baggage Makeup Area Space in which arriving and departing baggage is sorted and routed to appropriate destinations.

BAP Blast Analysis Plan

BHS Baggage Handling System

BIDS Baggage Information Display Systems

BMA Baggage Makeup Area

Boarding Gate The area from which passengers directly enplane or deplane the aircraft.

Cargo Property tendered for air transportation accounted for on an air waybill. All accompanied commercial courier consignments, whether or not accounted for on an air waybill, are also classified as cargo. Any property carried on an aircraft other than mail, stores and accompanied or mishandled baggage. Aircraft operator security programs further define the term "cargo."

Cargo Area All the ground space and facilities provided for cargo handling. It includes airport ramps, cargo buildings and warehouses, parking lots and roads associated therewith.

Carry-on baggage	An individual’s personal property that is carried into a designated Sterile Area or into an aircraft cabin and is accessible to an individual during flight
CBIS	Checked Baggage Inspection System
CBP	Customs and Border Protection (U.S.)
CBRA	Checked Baggage Resolution Area
CBRN	Chemical, Biological, Radiological, Nuclear
CBW	Chemical and Biological Weapon (or Chemical and Biological Warfare)
CCD	Charge-Coupled Device
CDG	Checkpoint Design Guidelines
CFR	Code of Federal Regulations (U.S.)
CHRC	Criminal History Records Check
Checked Baggage	Property tendered by or on behalf of a passenger and accepted by an aircraft operator for transport, which is inaccessible to passengers during flight. Accompanied commercial courier consignments are not classified as checked baggage.
Chem-Bio	Chemical and Biological
Concourse	A passageway for persons between the principal terminal building waiting area and the structures leading to aircraft parking positions.
CP	Command Post (typically, for purposes of this document, the Airport Emergency Command Post)
CPU	Central Processing Unit
Crisis Management Team	A group of individuals involved in managing a crisis to prevent, or at least contain, a crisis situation from escalating, jeopardizing safety and facilities, attracting unfavorable attention, inhibiting normal operations, creating a negative public image, and adversely affecting the organization’s viability.
Curbside Check-In	An area normally located along a terminal’s vehicle curb frontage where designated employees accept and check-in baggage from departing passengers. Designed to speed passenger movement by separating baggage handling from other ticket counter and gate activities. Allows baggage to be consolidated and moved to the screening process and to the aircraft more directly.
CUPPS	Common-Use Passenger Processing Systems
DVR	Digital Video Recorder
EDS	Explosives Detection System
EIA	Electronics Industry Alliance

Emergency Command Post A room or combination of rooms/facilities from which a Crisis Management Team commands and directs an event or incident, such as a natural disaster, terrorist event, hostage situation or aircraft disaster.

EMS Emergency Medical Services

EOC Emergency Operations Center (See also Emergency Command Post

EOD Explosive Ordnance Disposal—To render safe either improvised or manufactured explosive devices by the use of technically trained and equipped personnel.

EBSP Electronic Baggage Screening Program

Escort To accompany or monitor the activities of an individual who does not have unescorted access authority into or within a Secured Area or SIDA

ETD Explosives Trace Detection (or Detector)

ETD In the context of passenger scheduling, ETD means “estimated time of departure.”

Exclusive Area 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 49 CFR § 1546 has assumed responsibility under 49 CFR § 1542.111.

Exclusive Area Agreement An agreement between the airport operator and an aircraft operator that permits the operator to assume responsibility for specified security measures in 49 CFR § 1542.111. Does not include law enforcement responsibilities.

Explosives Military, commercial, or improvised compounds characterized by their ability to rapidly convert from a solid or liquid state into a hot gaseous compound with a much greater volume than the substances from which they are generated.

Explosives Detection System A system designed to detect the chemical signature of explosive materials, where the TSA has tested the system or devices against pre-established standards, and has certified that the system meets the criteria in terms of detection capabilities and throughput to detect in checked baggage, the amounts, types, and configurations of explosive materials as specified by TSA.

Explosives Trace Detection A device that has been certified by TSA for detecting explosive particles on objects intended to be carried into the Sterile Area or transported on board an aircraft. As used in this document, a device that detects tiny amounts of particle and/or vapor forms of explosives.

FAR Federal Aviation Regulation (U.S.)

FBO Fixed Base Operator

fc Footcandle

FCC Federal Communications Commission (U.S.)

FIDS Flight Information Display Systems

FIS Federal Inspection Services (U.S.)—U.S. Customs and Border Protection (CBP), U.S. Fish and Wildlife Service (FWS), and Public Health Service (PHS)

FSD TSA Federal Security Director

GA General Aviation

General Aviation That portion of civil aviation that encompasses all facets of aviation except commercial and military aircraft operators.

Ground Transportation Staging Area (GTSA) The location where taxis, limos, buses and/or other ground transportation vehicles are staged prior to the terminal.

Hazardous Material As defined in 49 USC § 5103 of the hazardous materials transportation law. Substances determined to be capable of posing an unreasonable risk to health, safety, and property when transported in commerce—also referred to as “dangerous goods” under international regulations.

Hijacking The exercising, or attempt to exercise, control over the movement of an aircraft by the use of force or threats, which, if successfully carried out, would result in the deviation of an aircraft from its regularly scheduled route.

HVAC Heating, Ventilation, and Air Cooling

IATA International Air Transport Association

ICAO International Civil Aviation Organization—a specialized agency of the United Nations whose objective is to develop the principles and techniques of international air navigation and to foster planning and development of international civil air transport.

ICE DHS Immigration and Customs Enforcement

ICS Individual Carrier System

ID Identification—use of methods such as access media, signs or markers to identify persons, vehicles and/or property

IEEE Institute of Electrical and Electronic Engineers

IESNA Illumination Engineering Society of North America

IETF Internet Engineering Task Force

Improvised Explosive Device (IED) A device that has been fabricated in an improvised manner and incorporates explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals in its design. Generally, an IED will consist of an explosive, a power supply, a switch or timer, and a detonator or initiator.

Incendiary Any substance that can cause a fire by ignition (flammable liquids, gases, or chemical compounds), or device that can be used to initiate a fire.

Indirect Air Carrier Any person or entity that undertakes to engage indirectly in air transportation of property, and uses the services of a passenger air carrier. This does not include the United States Postal Service (USPS) or its representative while acting on the behalf of the USPS.

Indirect Air Carrier Standard Security Program (ICASSP) A standard security program for indirect air carriers regulated in accordance with 49 CFR § 1548

Intermodal The use of two or more modes of transportation to complete the movement of a passenger or cargo from origin to destination; for example, cruise ship-to-aircraft (passenger), or aircraft-to-truck-to-rail-to-ship (cargo).

International Airport An airport used as a point of entry and departure for international air traffic, where the formalities incident to customs, immigration, public health, animal and plant quarantine and similar procedures are carried out.

IR Infrared

ISO International Standards Organization

Isolated Parking Position An area designated for the parking of aircraft suspected of carrying explosives or incendiaries to accommodate responding law enforcement and/or EOD personnel in search efforts.

ITU International Telecommunications Union

K-9 Canine Team—Dog teams used for explosives or other material detection.

kg Kilogram, 1000 grams or 2.2 pounds; (a typical spray can holds approximately 300 grams).

LAN Local Area Network

Law Enforcement Officer An individual authorized to carry and use firearms, vested with such police power of arrest as determined by federal law and state statutes, and identifiable by appropriate indicia of authority, and who is trained and commissioned to enforce the public criminal laws of the jurisdiction(s) in which he or she is commissioned.

Landside That area of an airport and buildings to which both traveling passengers and the non-traveling public have unrestricted access. (See also Non-Restricted Area.)

LED Light-Emitting Diode

LEO Law Enforcement Officer

LVIED Large Vehicle IED

Metal Detector (also magnetometer) An electronic detection device approved by the TSA to detect metal on persons desiring access beyond the screening point. May be walkthrough or handheld type.

Micron 0.001 millimeter or 0.00004 inches

Movement Area The runways, taxiways, and other areas of an airport used for taxiing, takeoff, and landing of aircraft, exclusive of loading ramps and aircraft parking areas.

NAS Network Attached Storage

NEC National Electrical Code

NFPA National Fire Protection Association (U.S.)

Off-Airport Facility Refers to a passenger or cargo transport terminal at an urban population center at which processing facilities are provided prior to arrival at airport.

On-Screen Alarm Resolution EDS tools/functions that can be used to resolve or suspect EDS alarm objects.

OSR On-Screen Resolution

Perimeter The outer boundary of an airport, also a boundary that can separate areas controlled for security purposes from those that are not.

Person An individual, corporation, company, association, firm, partnership, society, joint-stock company, or governmental authority. It includes a trustee, receiver, assignee, successor, or similar representative of any of them.

PGDS *Planning Guidelines and Design Standards* (for Checked Baggage Inspection Systems)

PIN Personal Identification Number

POE Port-of-Entry (FIS)

Private Charter Any aircraft operator flight—(1) For which the charterer engages the total passenger capacity of the aircraft for the carriage of passengers; the passengers are invited by the charterer; the cost of the flight is borne entirely by the charterer and not directly or indirectly by any individual passenger; and the flight is not advertised to the public, in any way, to solicit passengers; (2) For which the total passenger capacity of the aircraft is used for the purpose of civilian or military air movement conducted under contract with the government of the United States or the government of a foreign country

PTZ Pan-Tilt-Zoom

Public Area That portion of the airport that includes all public real estate and facilities other than the AOA and those Sterile Areas downstream of security screening stations

RAID Redundant Array of Independent Disks

Record Includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term record also includes any draft, proposed, or recommended change to any record.

RF Radio Frequency

RFI Radio Frequency Interference

RFID Radio Frequency Identification

RTCA Radio Technical Commission for Aeronautics

SAN Storage Area Network

SARP *Standards and Recommended Practices* (ICAO)

Screening The application of technical or other means which are intended to identify and/or detect weapons, explosives or other dangerous devices, articles or substances which may be used to commit an act of unlawful interference. The checked baggage screening functions are: (1) EDS screening, (2) ETD screening, (3) combination of EDS/ETD, and (4) physical inspection.

Screening Location Each site at which individuals, accessible property, or checked baggage is inspected for the presence of explosives, incendiaries, weapons, or other prohibited items. These include the screening checkpoint or boarding gate where individuals and accessible property are inspected with metal detectors, x-ray devices, and other methods; concourse, lobby or baggage make-up areas where checked baggage is inspected with an EDS and/or ETD; and locations where cargo is inspected.

Secured Area 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 49 CFR 1546 enplane and deplane passengers and sort and load baggage, and any adjacent areas that are not separated by adequate security measures.

Security Areas Areas defined by and subject to security requirements and regulation; e.g., AOA, ATSP Area, Exclusive Use Area, Secured Area, SIDA, Sterile Area.

Security Contingency Plan A plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management.

Security Directive A document issued by TSA to notify aircraft operators and/or airport operators of specific credible threats, and measures required for response.

Security Identification Display Area (SIDA) A portion of an airport, specified in the ASP, in which security measures specified in 49 CFR § 1542 are carried out. This area includes the Secured Area, and may include other areas of the airport.

Security Program A program or plan and any amendments, developed for the security of (1) An airport, aircraft, or aviation cargo operation; (2) A maritime facility, vessel, or port area; or (3) A transportation-related automated system or network for information processing, control, and communications.

Security Parking Area An aircraft stand where aircraft threatened with unlawful interference may be parked pending resolution of the threat. Also known as a "hot spot."

Shield Alarm An EDS alarm caused by substances too dense for x-rays to penetrate, and which EDS is unable to analyze.

Should For the purpose of this document, this word is defined as a recommendation or that which is advised but not required.

SOC Security Operations Center

SONET Synchronous Optical Network

SSCP Security Screening Checkpoint—A checkpoint area established to conduct security screening of persons and their possessions prior to their entering a Sterile or Secured Area.

SSI Sensitive Security Information, as described in 49 CFR § 1520.5

Stand-Alone Systems A non-integrated checked baggage screening system where the passenger checks his or her baggage with the aircraft operator in the airport lobby for screening by an EDS and/or ETD.

Sterile Area A portion of an airport defined in the ASP that provides passengers access to boarding aircraft, and to which the access generally is controlled by TSA, or by an aircraft operator or a foreign air carrier, through the screening of persons and property. Generally, that area between the passenger screening checkpoint and the aircraft boarding areas.

TCU Threat Containment Unit—a wide variety of devices used to contain wholly or in part the blast effects of an explosive device. TCUs may be stationary, or may be part of a system by which an explosive device may be transported.

Terminal A building or buildings designed to accommodate the enplaning and deplaning activities of aircraft operator passengers.

Threat A threat is any indication, circumstance, or event with the potential to cause loss of or damage to an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to United States interest. There are six primary sources of threats: Terrorist, Criminal, Insider, Foreign Intelligence Service, Foreign Military, and Environmental—as defined by the CIA's Analytical Risk Management Program.

Through-the-Fence Agreement	Allows an off-airport aircraft owner at an off-airport property to use a cross-boundary taxiway to access the airport’s taxiway-runway system.
Transportation Security Regulation(s)	The regulations issued by the TSA, in Title 49 of the Code of Federal Regulations, Chapter XII, which includes parts 1500 through 1699.
TSNM	Transportation Sector Network Management (TSA)
TTAC	Transportation Threat Assessment and Credentialing (TSA)
Unescorted Access Authority	The authority granted by an airport operator, an aircraft operator, foreign air carrier, or airport tenant under §§ 1542, 1544, or 1546, to individuals to gain entry to, and be present without an escort in, Secured Areas and SIDAs of airports.
UAS	Unmanned Aircraft Systems
VBIED	Vehicle Borne Improvised Explosive Device
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
Vulnerability	A weakness in physical structures, personnel protection systems, processes, or other areas that may be exploited by criminals or terrorists.
Vulnerability Assessment	Any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area; vessel, aircraft, train, commercial motor vehicle; or pipeline; or a transportation-related automated system or network, to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A vulnerability assessment may include proposed, recommended, or directed actions, or countermeasures to address security concerns.
Vulnerable Area/Point	Any facility or area at an airport, which, if damaged or otherwise rendered inoperative, would seriously impair the functioning of an airport.
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WMD	Weapons of Mass Destruction (typically includes chemical, biological, radiological, and nuclear weapons).
WTMD	Walk-Through Metal Detector

APPENDIX A: Risk and Vulnerability Assessments

1. Introduction

Security is a process of risk management, identifying threats, and assessing how vulnerable the airport might be to various types of threats and scenarios including their consequential actions.

Threats are specific activities that are likely to damage the airport, its facilities, its personnel or its patrons. Threats range from the extreme of terrorist-initiated bombs or hostage-taking to more common events such as theft of services, pick-pocketing, graffiti and vandalism. Those responsible for identifying and assessing threats and vulnerabilities must not only measure the degree of potential danger, but the chances of that particular danger actually occurring; define what preparations and actions are needed to mitigate such events, and then consider and prioritize what resources are available for response and recovery. This also must consider the possibility of multiple simultaneous events that may or may not be related.

Threats and vulnerabilities cover a wide array of events, virtually none of which can be totally eliminated while still operating the system. Since no system can be rendered totally secure, once threats and vulnerabilities are identified, their impact on the total system must be assessed to determine whether to accept the risk of a particular danger, and the extent to which corrective measures can eliminate or reduce its severity.

Vulnerability is the susceptibility of the airport and its systems to a particular type of security hazard. Vulnerabilities are commonly prioritized through the creation of scenarios that pair identified assets and threats. A risk analysis must be undertaken to determine which vulnerabilities take the highest priority. This is best done during the initial ConOps process, when operational requirements are established, and should be extended into the design and construction of a facility, in its technological systems, since an increased priority in one area typically means another area will receive less attention. Also wielding considerable influence in the design decisions is the way a facility is operated (e.g., security procedures and practices or administrative and management controls, including staffing considerations).

An airport vulnerability assessment is a tool for determining the extent to which an airport facility may require security enhancements. It serves to bring security considerations into the mix early in the design process rather than as a more expensive retrofit.

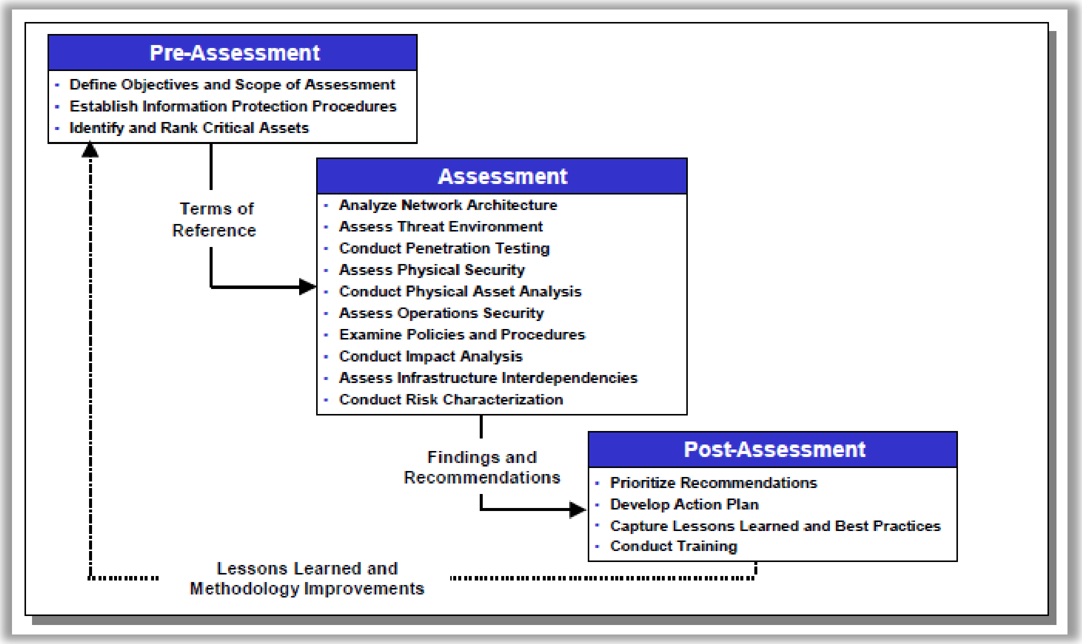
2. The Assessment Process

Threat and vulnerability assessments provide an analytical process for considering the likelihood that a specific threat will endanger the targeted facilities and their systems. Using the results of a capabilities assessment, threat and vulnerability analyses can also identify activities to be performed to (a) reduce the risk of an attack and (b) to mitigate the consequences of an attack.

Assessments typically use a combination of quantitative and qualitative techniques to identify security requirements, including the historical analyses of past events, intelligence assessments, physical surveys, and expert evaluation. When the risk of hostile acts is greater, these analytic methods may draw more heavily upon information from intelligence and law enforcement agencies regarding the capabilities and intentions of the aggressors.

Assessments may be model-based. Several types are available for an airport to use including models developed by DHS, TSA, and the Energy Department process diagrammed in Figure A-1.

Figure A-1. Vulnerability Assessment Phases


Pre-Assessment
Define Objectives and Scope of Assessment
Establish Information Protection Procedures
Identify and Rank Critical Assets
Terms of Reference
Assessment
Analyze Network Architecture
Assess Threat Environment
Conduct Penetration Testing
Assess Physical Security
Conduct Physical Asset Analysis
Assess Operations Security
Examine Policies and Procedures
Conduct Impact Analysis
Assess Infrastructure Interdependencies
Conduct Risk Characterization
Findings and Recommendations
Post-Assessment
Prioritize Recommendations
Develop Action Plan
Capture Lessons Learned and Best Practices
Conduct Training
Lessons Learned and Methodology Improvements

Source: US Dept. of Energy

When analyzing the results of the vulnerability assessment, considerations should be balanced and should implement enhanced security requirements in accordance with those security systems, methods and procedures that are required by law or regulation, including ATSA, the CFRs as well as industry-recommended best practices.

Effective assessments typically include five elements, each of which will be discussed in this section:

- Asset analysis
- Target or threat identification
- Vulnerability assessment
- Consequence analysis (scenarios)
- Counter-measure recommendation, including recovery

DHS has also recently adopted a new tool originally developed to address risks in environmental policy, but adaptable in other disciplines, called the Deliberative Method for Ranking Risk, to aid in strategic planning for security. It is discussed in findings published in Homeland Security Affairs and the Journal of Homeland Security and Emergency Management in response to a National Academy of Sciences recommendation that the DHS adopt qualitative risk assessments as part of the strategic planning process.

a. Asset Analysis

For security purposes, assets are broadly defined as people, information, and property. In public transportation, the people include passengers, employees, visitors, contractors, vendors, nearby community members, and others who come into contact with the system. Information includes operating and maintenance procedures, air and ground vehicles, terminal and tenant facilities, power systems, employee information, information systems and computer network configurations and passwords, et al.—many of which will involve proprietary information.

In reviewing assets, the airport system should prioritize which among them has the greatest consequences for people and the ability of the airport and its systems to sustain service. These assets may require higher or special protection from an attack. In making this determination, the airport operator may wish to consider:

- The value of the asset, including current and replacement value;
- The value of the asset to a potential adversary;
- Where the asset is located and how, when, and by whom an asset is accessed and used; and
- What is the impact, if these assets are lost, on passengers, employees, public safety organizations, the general public and airport operations?

b. Threats

A threat is any action with the potential to cause harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services. System facility threats include a number of hostile actions that can be perpetrated by criminals, disgruntled employees, terrorists, and others, including the possibility of ordinary carelessness or incompetence by improperly trained operational personnel.

Threat analysis defines the level or degree of the threats against a facility by evaluating the capability, intent, motivation, and possible tactics of those who may carry them out. The process involves gathering historical data about hostile events and evaluating which information is relevant in assessing the threats against the facility.

Some of the questions to be answered in a threat analysis:

- What factors about the system invite potential hostility?
- How conspicuous is the transportation facility or vehicle?
- What political event(s) may generate new hostilities?
- Have facilities like this been targets in the past?

Possible methods of carrying out hostile actions in the transportation environment are depicted in Table A-1. Historical examples are provided for reference and consideration, as well as to illustrate the types of weapons typically used in these attacks.

Table A-1. Examples of Terrorist Attacks and Weapons

Type of Attacks	Historical Examples	Type of Weapons
Explosives and Firearms	2016 Bombings and gunfire in the Istanbul Ataturk International Airport terminal kills 41, injures 239	Firearms and suicide vests, or IEDs
Explosives and Incendiaries	2016 Bombings in the Brussels International Airport and Maalbeek metro station kills 32, injures 340 2016 Bus bombing in Jerusalem injures 20 2015 Metrojet bombing over Egypt kills 224 2014 Bombing of a tourist bus in Sinai kills four 2013 Attempt to detonate a vehicle bomb at Wichita Mid-Continent Airport, Kansas 2012 Bomb attack on a bus in Bulgaria kills seven 2011 Bomb at Moscow Airport-kills 36, injures 180	Suicide bombs, IEDs or incendiary devices
	2016 Car bomb attack at a bus and subway hub in Ankara, Turkey kills 37, injures 125 2016 Somalia Daallo Airlines inflight bomb attack 2011 Plot to attack the Pentagon and the Capitol with large model aircraft packed with explosives 2011 Bomb bus station- Jerusalem kills 1, injures 39	IEDs
	2010 Explosive devices hidden in printer toner cartridges on all-cargo flights from Yemen	IEDs
	2010 Incendiary devices mailed to Maryland and Washington D.C. area facilities	Incendiary devices
	2009 Attempt to detonate device onboard Northwest Airlines Flight 253	Concealed body-worn plastic explosives
	2007 Attack on Glasgow International Airport 2007 Plot to bomb fuel tanks at JFK Airport 2005 Bomb subway in London kills 50, injures 700+	Suicide incendiary car bomb Incendiary or IEDs
	2001 Attempt to detonate explosive device onboard American Airlines Flight 63	Concealed plastic explosives in worn shoe
	2001 World Trade Center and Pentagon aircraft attacks kill 2,996, injure 6000+ 1995 Oklahoma City Murrah Federal Building car bombing kills 168, injures 650+	Proximity bombs, incendiary & secondary devices
Stand-Off	2015 Mortar attack on Sabiha Gökçen International Airport in Istanbul, Turkey 2001 Tamil Tiger mortar attack and bombing of Sri Lanka's International Airport	Anti-tank rockets, mortars
Cyber	2015 *Anonymous* attacked Narita and Chubu International Airport websites in Japan	Worms, Viruses, Denial of Service Programs
Chemical, Biological, Radiological, & Nuclear	1995 Aum Shinrikyo Sarin agent release in Tokyo Subway kills 12, injures 5,500+	Aerosolized CBRN

Source: TranSecure, Inc.

c. Vulnerabilities

Using these scenarios, transportation agencies can evaluate the effectiveness of their current policies, procedures, and physical protection capabilities to address consequences.

d. Consequence Analysis (Scenarios)

Scenario analysis requires an interpretive methodology that encourages role-playing by the local transportation personnel, emergency responders, and contractors to brainstorm ways to attack the system, because they know the system and its vulnerabilities best. By matching threats to critical assets, transportation personnel can identify the capabilities required to support specific types of attacks. This activity promotes awareness and highlights those activities that can be performed to recognize, prevent, and mitigate the consequences of attacks. Table A-2 lists examples of likely threats to airports.

Table A-2. Examples of Likely Threat Scenarios

Assets	Most Probable Threats
Terminals	• High Yield vehicle bomb near terminal • Low yield explosive device in terminals • Hi-jacking, hostage or barricade situation in terminal • Chemical, biological or nuclear release in terminal • Secondary explosive directed at emergency responders
Fuel Storage Facilities	• Explosives detonated in/near fuel facilities
Security Operations Centers	• Physical or cyber-attack on dispatch system • Armed assault, hostage or barricade situation • Explosive device in/near Operations Control Center • Sabotage of vehicle or maintenance facility

Source: TranSecure, Inc.

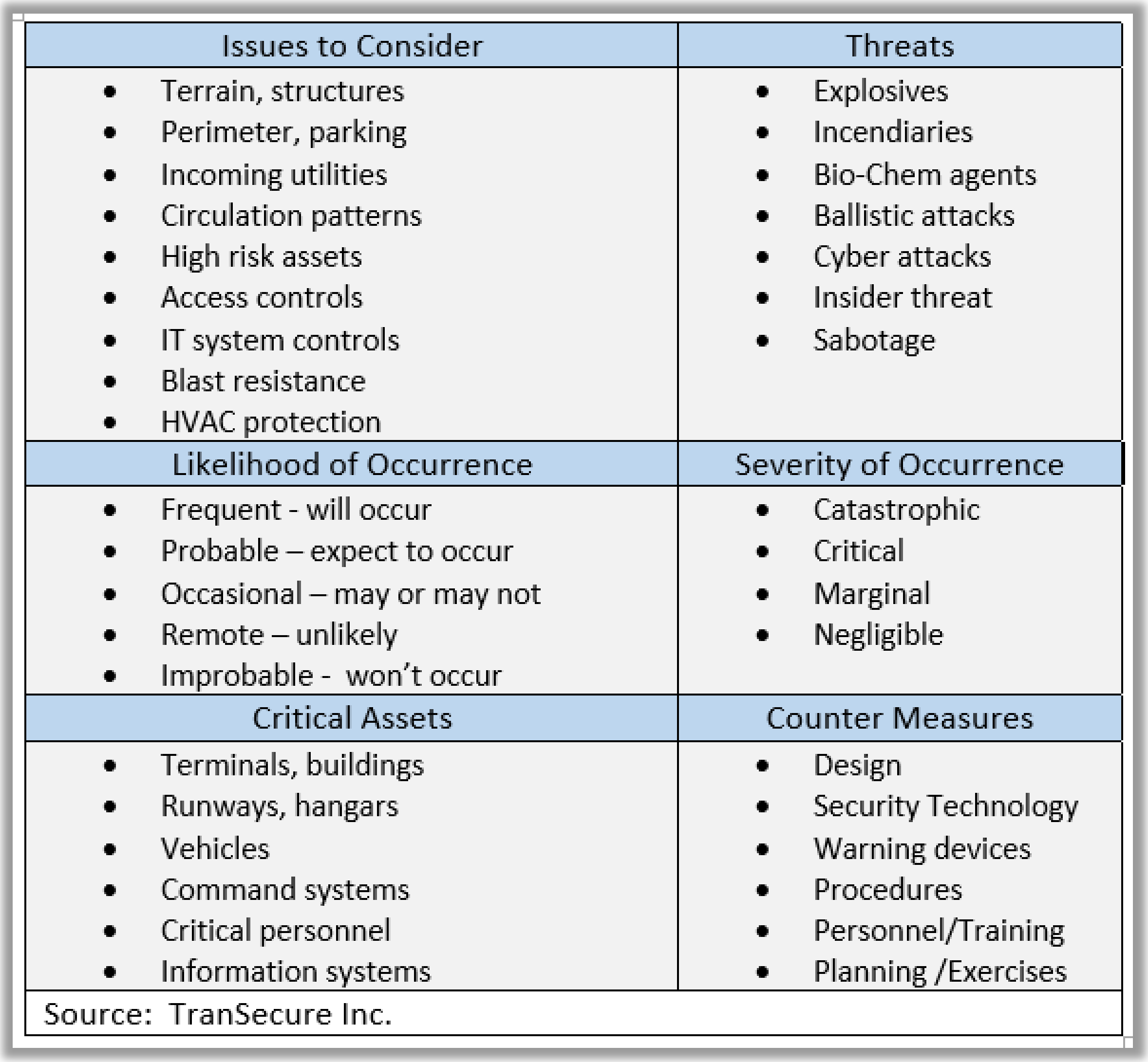
The airport operator should also consider the range of perpetrators, such as political terrorists, radicals, right-wing extremists, disgruntled employees, disturbed copycats, and others.

When conducting the scenario analysis, the system may choose to create chronological scenarios (event horizons) that emphasize the worst credible scenario as opposed to the worst case scenario.

e. Consequences

Consequences are assessed both in terms of severity of impact and probability of loss for a given threat scenario. Table A-3 shows one process for accomplishing this. For each scenario, airport planners and designers should attempt to identify the costs and impacts using a standard risk level matrix, which supports the organization of consequences into categories of high, medium, and low.

Table A-3. Scenario Evaluation Criteria



Issues to Consider	Threats
• Terrain, structures	• Explosives
• Perimeter, parking	• Incendiaries
• Incoming utilities	• Bio-Chem agents
• Circulation patterns	• Ballistic attacks
• High risk assets	• Cyber attacks
• Access controls	• Insider threat
• IT system controls	• Sabotage
• Blast resistance	
• HVAC protection	
Likelihood of Occurrence	**Severity of Occurrence**
• Frequent - will occur	• Catastrophic
• Probable – expect to occur	• Critical
• Occasional – may or may not	• Marginal
• Remote – unlikely	• Negligible
• Improbable - won't occur	
Critical Assets	**Counter Measures**
• Terminals, buildings	• Design
• Runways, hangars	• Security Technology
• Vehicles	• Warning devices
• Command systems	• Procedures
• Critical personnel	• Personnel/Training
• Information systems	• Planning /Exercises
Source: TranSecure Inc.	

Scenario-based analysis is not an exact science but rather an illustrative tool demonstrating potential consequences associated with low-probability to high-impact events. To determine the system's actual need for additional countermeasures, and to provide the rationale for allocating resources to these countermeasures, the scenarios can be used to pinpoint the vulnerable elements of the critical assets and make evaluations concerning the adequacy of current levels of protection. Scenarios with vulnerabilities identified as high may require further investigation.

Examples of vulnerabilities that may be identified from scenario-based analysis include the following:

- Accessibility of surrounding terrain and adjacent structures to unauthorized access (both human and vehicular);
- Site layout and elements, including perimeter and parking that discourage access control, support forced or covert entry, and support strategic placement of explosives for maximum damage;
- Location and access to incoming utilities (easy access for offenders); lines of sight for weapons attack;
- Building construction with respect to blast resistance (tendency toward progressive collapse, fragmentation, or no redundancy in load bearing);
- Sufficiency of lighting, locking controls, access controls, alarm systems, and venting systems to support facility control; and
- IT and computer network ease-of-penetration.

At the conclusion of the scenario-based analysis, the airport operator should have assembled a list of prioritized vulnerabilities for its top 10 percent critical assets. These vulnerabilities may be organized into the following categories, which should be documented in a confidential report:

- Lack of planning;
- Lack of coordination with local emergency responders;
- Lack of training and exercising; and
- Lack of physical security (access control, surveillance; blast mitigation, or chemical, biological, or radioactive agent protection).

3. Developing Countermeasures

Based on the results of the scenario analysis, the airport operator can identify countermeasures to reduce vulnerabilities.

Effective countermeasures typically integrate mutually supporting elements.

- Physical protective measures designed to reduce system asset vulnerability to explosives, ballistics attacks, cyber-attacks, and the release of chemical, biological, radiological, or nuclear (CBRN) agents.
- Procedural security measures, including procedures to detect and mitigate an act of terrorism or extreme violence and those employed in response to an incident that does occur.

In identifying these measures, the airport should be able to answer the following questions.

- What are the operational priorities and budgetary constraints?
- What different countermeasures are available to protect an asset?
- What is the varying cost and effectiveness of alternative measures?

In many cases, there is a point beyond which adding countermeasures will raise costs without appreciably enhancing the protection afforded.

One countermeasure strategy is to place the most vulnerable assets within concentric levels of increasingly stringent security measures. For example, an airport's Security Operations Center (SOC) should not be placed right next to the building's reception area; it should be located deeper within the building so that to reach the control center, an intruder would have to penetrate numerous rings of protection such as a fence at the property line, a locked exterior door, an alert receptionist, an elevator with key-controlled floor buttons, and a locked door to the control room.

Other prevention strategies involve cooperation with law enforcement agencies, security staff in other systems, and industry associations in order to share threat information. It is useful to know whether other transportation systems in an area have experienced threats, stolen uniforms or keys, or a particular type of criminal activity, in order to implement appropriate security measures.

In the assessment, the team may consider both passive and active strategies for identifying, managing, and resolving threats to the system's operation. Team members should provide appropriate expertise in both these strategies.

Passive strategies include all security and emergency response planning activity, outreach with local law enforcement, training, evacuation and business continuity and recovery plans, employee awareness, public information, and passenger training. Passive responses also include security design strategies, supported by crime prevention through environmental design and situational crime prevention methods, such as landscaping, lighting, and physical barriers (planters, bollards, road blockers, forced entry rated fencing, et al.).

Active strategies include security technology, such as electronic access control, intrusion detection, CCTV, digital recorders, emergency communications systems, and chemical agent or portable explosives detectors. Active systems also include personnel deployment.

It is important to consider the entire lifecycle cost when evaluating security solutions. Technology options may require a substantial one-time investment, supported by fractional annual allocations for maintenance and vendor support contracts. Personnel solutions are generally more expensive.

APPENDIX B: Airport Blast Protection

1. Introduction

Recent overseas attacks have provided added impetus to protect passengers and personnel at U.S. airports and have led to changes in law and mandated security directives, many of which have affected how airports operate during heightened threat levels. It has become increasingly important to consider how best to plan, design and construct airport terminals, roadways, and essential ancillary facilities with blast protective measures in mind. See Title 6 USC § 607 and § 609; Title 49 USC § 44903(c) and (h); § 44904(a) through (e); § 44912(a) and (b).

Over the next several years, the potential threats and Federal security mandates at airports will no doubt continue to evolve. Therefore, it is very beneficial have a flexible airport layout and design that can be readily adapted to changing rules and threats. Furthermore, it is prudent to consider the impacts, both financial and operational, of having to cope with the restrictions imposed during high threat levels that occur often or for extend durations. These impacts should not be taken lightly. Airports that are ill-equipped to operate during high threat levels oftentimes face large vehicular traffic backups and long lines at passenger screening portals, both of which add considerable time to a passenger's point-to-point commute, and affect the airport's ability to deal with larger, longer-term crowds.

a. Why Airports?

There are countless potential terrorist targets ranging from commercial buildings to specific social, religious, and political groups. Transportation facilities such as airports, subways, train stations, and bus stations are all potential targets of terrorism not only because they are vital to a stable economy and to the operation of countless businesses, but they are very visible, accessible, high-profile facilities filled with a high density of people.

The FAA Extension, Safety, and Security Act of 2016 (P.L. 114-190) contains Title III Aviation Security which includes references to "non-Secure" and "non-Sterile" Areas and "security events at public locations, including airports and mass transit systems" that give a nod to the 2016 events in Brussels and Istanbul and their pathways of attack.

- Section 3602 adds a new subparagraph to the list of law enforcement terrorism prevention activities under (a)(2) of Title 6 U.S.C. § 607 on terrorism prevention that already includes target hardening, threat recognition and terrorist interdiction: "(E) training exercises to enhance preparedness for and response to mass casualty and active shooter incidents and security events at public locations, including airports and mass transit systems."
- Section 3603 makes changes to Title 6 U.S.C. § 609 on homeland security grants to high risk urban areas and States for terrorism prevention, protection and response to make funds available to DHS for grants for "enhancing the security and preparedness of secure and non-secure areas of eligible airports and surface transportation systems." Both insertions into the law covering domestic security are designed to provide funds to mitigate the threat against U.S. airports and other domestic transportation hubs from attacks in the public area from the curb to the ticket counter that lie outside of traditional security screening checkpoints.

b. Risk Management

Protection/mitigation from IED and VBIED threats can be provided in many forms:

- Security design: using cameras, sensors, alarms, K-9, and patrols, etc.;
- Standoff: separation between a potential bomb source and certain targets;
- Physical protection: using gates, barriers, blast-hardened columns, blast debris screens, and blast-resistant windows, etc.;
- Risk acceptance: through prioritization of protective measures based upon a vulnerability assessment, implementation cost, and overall airport security plan; and
- Blend of all of the above: in an integrated security plan that combines mobile security, standoff, physical protection, and risk acceptance into an overall solution.

While it is important to consider how to provide some measure of blast protection at airports, it is also important to recognize that it is not feasible or cost-effective to fully mitigate all potential VBIED threats. Inherently, by their nature and usage, airports must be convenient to use and process thousands of passengers in a short timeframe. Thus, like driving an automobile on high speed interstate highways, some amount of "risk acceptance" is necessary. Likewise, while it is physically possible to design an airport more like a bomb shelter or fortress, this would severely compromise airport operations, cost substantial amounts of money, and be unacceptable to the traveling public… and still not be entirely risk-free. Each airport operator is left with making important and locally unique decisions on how best to provide reasonable and prudent security and effective blast protection while weighing the effectiveness, cost, and impact on airport operations.

c. Planning Facility Blast Protection

Security planning should be an integral and early part of all projects undertaken at an airport. Security planning should include performing periodic vulnerability assessments of all facilities and the airport site, as well as evaluating the airport security program to confirm that Federal, State, and local standards have been met.

At first glance, many blast protection measures seem to focus on protecting airport facilities, such as the terminal building, from the devastating effects of a bomb blast. However, the real priority is to protect the passengers and personnel at airports. Providing blast protection for the facility is simply a means to saving lives in the event that a bombing occurs. Loss of life due to a terrorist bombing reduces significantly if the building remains standing and does not collapse.

A high level of security is achieved when the airport layout and terminal design complement the airport security plan. Having airport roadways, parking, and terminals positioned and designed with security in mind allows the airport to operate more safely and effectively—even during high threat levels. Furthermore, incorporating blast resistant features during the initial design costs less and blends with the overall building architecture much better than costly retrofit of a facility after the fact.

2. Common Airport Blast Protection Issues

The following is a summary of common vulnerability issues and recommended methods to physically harden airport facilities. The suggested security enhancements are voluntary upgrade options for an airport to consider. One must recognize that it is impossible to protect everyone from every conceivable threat. This is especially true when protecting public facilities, such as airports, that regularly allow thousands of people and vehicles that have not been screened for weapons or explosives to be in or near the facilities. However, with some planning, one can identify vulnerable areas and prioritize options to mitigate those threats.

a. Level of Blast Protection

In general, the objective for protecting airports is to provide a “medium” level of blast protection, recognizing that a significant degree of damage to a facility might occur, but the structure will be reusable and remain standing after most conceivable blasts. Some casualties likely will occur, assets probably will be damaged, and some building elements other than major structural members may require replacement.

In general, it is recommended to implement those security enhancements that protect the primary structure (beams and columns) from catastrophic damage first. All other enhancements are secondary to this. As an example, hardening the windows at a terminal perimeter offers little to no protection if the adjoining columns are destroyed from the bomb blast.

b. Common Vulnerabilities

- Roadways

  a) The roadways that surround airport terminals are designed to allow convenient passenger access. However, passenger convenience is often contrary to good security planning. Vehicles that enter airport “landside” property typically are not usually inspected, weighed, or screened except during high threat levels. Restricting or monitoring vehicles that enter landside areas of the airport can be accomplished some distance from the terminal building. Many security guidelines recommend that vehicle barriers be installed that will stop the threat vehicle at locations far enough from the facility to prevent catastrophic damage and minimize loss of life.

  b) Many airports have multi-level roadways (refer to Figure B-1) that are not physically protected from vehicular attacks or bomb blasts. Airports should consider hardening these columns to prevent severe damage due to vehicular impact or VBIED attacks.

  c) The approach roadways, by nature, are in close proximity to the terminal buildings, leaving the buildings vulnerable to vehicular impacts and vehicle bombs (refer to Figure B-2 and Figure B-3).

Figure B-1. Elevated Roadway

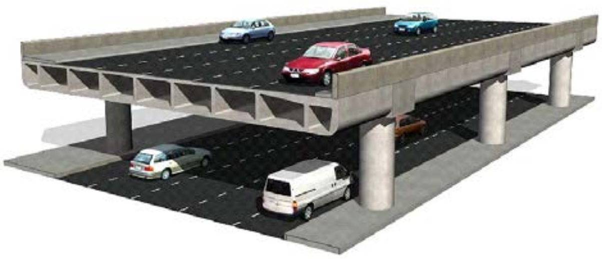
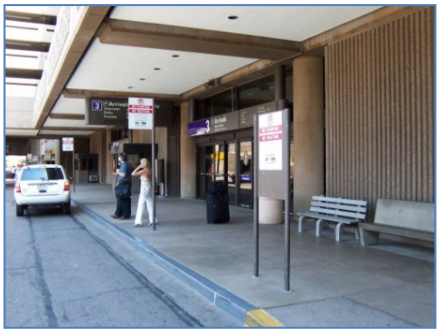


Figure B-2. Curbside Drop-Off at Ticketing Level

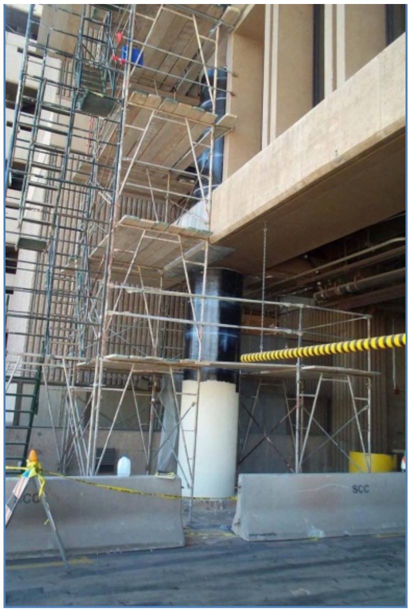


Source (B-1–B-5): Magnusson Klemencic Associates (MKA)

- Terminal Perimeter

Figure B-3. Curbside Pickup at Baggage Claim Level

Figure B-4. Wrapping Process—Kevlar-Carbon Fiber Wrap



a) Most exterior windows and doors are not designed to resist bomb blasts. Many security design guidelines recommend that exterior window systems (glazing, frames, anchorage to supporting walls, etc.) be hardened to mitigate the potentially lethal effects of flying glass following a small explosion. However, unlike other secure facilities, hardening the glazing at airport facilities offers limited protection against bombers that are able to flank around the hardened façade simply by walking through the entry doors with unscreened luggage in tow.

b) The columns and beams that support the terminal floors and roof structures often are not designed to resist bomb blasts. The GSA recommends that new construction be designed for the loss of one column for one floor above grade at the building perimeter, without progressive collapse. Alternatively, the columns shall be sized, reinforced, or protected so that the threat charge will not cause the column to be critically damaged. Refer to Figure B-4 for an example of column hardening by wrapping process.

c) Many large vehicles can gain uninspected access to terminal properties on either the landside or airside. These include delivery trucks, refuse trucks, construction trucks, and fuel trucks. Several thousand pounds of explosive material can be secreted in these vehicles, and since they are very difficult to visually inspect, they have relatively open access to deliver their bulk threat to any part of an airport.

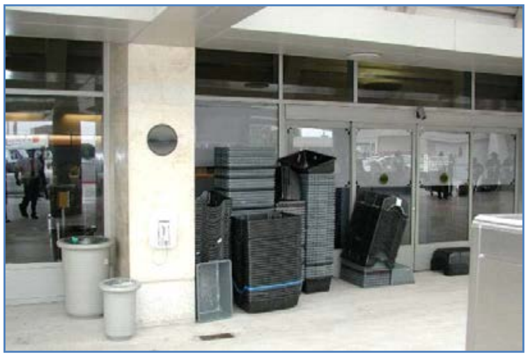
d) The exterior terminal doors often are not protected from vehicular attack.

e) Exterior trash containers and mail receptacles often are not explosion resistant. Receptacles should not be attached to columns or constructed of materials that would become dangerous shrapnel if a bomb is discharged within the container, such as aggregate concrete planters. Providing blast resistant trash containers at airports offers very minimal blast protection because countless passengers enter the landside area of the terminal with unscreened baggage; thus, the luggage itself provides ample opportunity to hide an IED.

f) There often are areas at curbside, such as luggage check-in counters and kiosks that could conceal explosive devices (refer to Figure B-5), and should be avoided. This includes benches, booths, planters, landscaping, etc. Avoid landscaping and furniture that permits concealment of criminal activity or obstructs the view of security personnel or closed-circuit television.

- Terminal Landside

Figure B-5. Potential Concealment Area at Ticketing Level

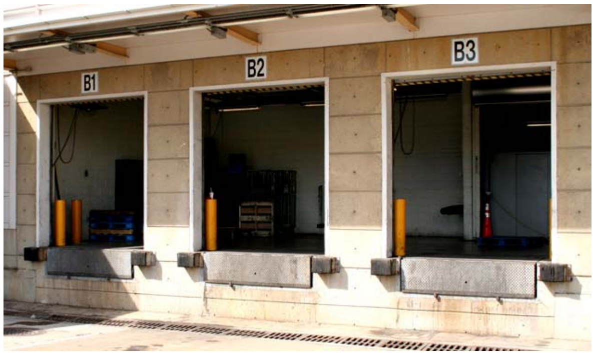


a) Passenger baggage presents a common challenge in an airport environment. It affords a potential bomber the opportunity to carry up to 75 pounds or more of explosives inside a terminal without much scrutiny—especially in terminals that service international flights, where passengers typically travel with oversized luggage. In addition, baggage claim areas offer a prime target of opportunity in airports where the area does not have controlled access. Uninspected baggage can be easily introduced in these environments, where it can remain until large crowds gather from an incoming flight.

b) Many public restrooms are located in landside non-secure areas. Although they are common in airports, such public restrooms, service spaces, or unscreened access to stairwells in landside non-secure locations should be avoided because these areas could conceal criminal activities or explosive devices.

c) Loading docks and shipping/receiving areas are not often designed to resist bomb blasts. Some security guidelines recommend that loading docks and shipping/receiving areas be at least 50 feet from utility rooms, utility mains, and service entrances such as electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc. Furthermore, when loading docks are located such that vehicles are driven or parked under the building (refer to Figure B-6), the airport operator should consider hardening the area to resist bomb blasts, and the room should be "vented" outward.

Figure B-6. Loading Dock



Source: MKA

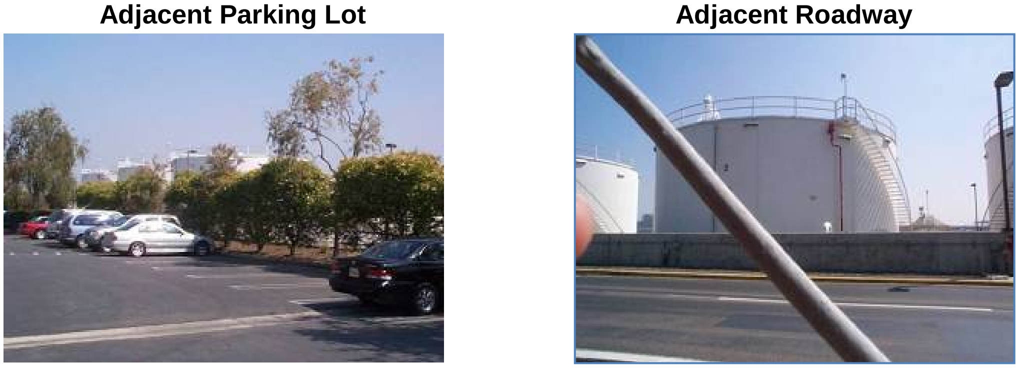
d) While it is convenient for passengers, the location of parking areas adjacent to the terminal area is not a preferred location from a blast-protection perspective. A blast analysis should be performed to justify parking within 300 feet of the terminal during elevated threat levels.

- Fuel Facility

a) The fuel farms that service the airport are often vulnerable. For example, there may be an uncontrolled parking lot that is not owned by the airport, which is adjacent to the fuel facility. (Refer to Figure B-7.)

b) The main power for the airport complex should be provided with redundant power and emergency power. Avoid placing substations adjacent to public roadways.

Figure B-7. Fuel Facility Power Substation



Source: MKA

- Air Traffic Control Tower

Figure B-8. ATC Tower

The International Code Council defines Air Traffic Control Towers (ATCT; Figure B-8) as essential facilities. Obviously, the airport must have a fully functional ATCT in order to operate. Public parking adjacent to an ATCT may be limited by FAA regulations. Methods to protect the ATCT structure and cab from blast and ballistic attack also should be considered.

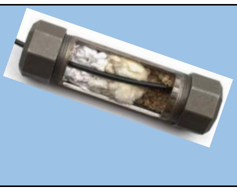
c. Critical Building Components

Many building components are critical to the continuous operations of an airport. Other components are critical to emergency operations. These components should be protected as much as possible from sabotage and other catastrophic events. These components include the following:

- Emergency generators - fuel systems, fire sprinkler, water supply
- Fuel storage and delivery systems
- Main switchgear
- Telephone distribution/ main switchgear
- Fire pumps
- Building security control centers
- UPS systems for critical functions
- Main refrigeration systems
- Elevator machinery and controls
- Shafts for stairs, elevators, and utilities
- Emergency power distribution
- Navigation/ communications equipment
- Airport Emergency Command Post
- Electric substations (local/regional)

In general, different types of explosive materials have different equivalencies to similar quantities of TNT, the standard by which they are measured (refer to Table B-1).

Table B-1. TNT Equivalents

A terrorist's skill in constructing IED or Vehicle-Borne IEDs (VBIED) is likely to influence the type of attack it might execute. Bomb makers with only rudimentary skills may be restricted to assembling basic devices. A skilled journeyman bomb maker may have the competence needed to build a range if IEDs from small to large that are highly concealable or have advanced capabilities such as multiple triggering methods, directional blasts, or increased blast effect. Two hundred kilograms of explosive can do extensive damage to buildings and personnel.			
			
200 Pipe Bombs @ 1 KG each	20 Suicide Vests @10 KG each	2 Small VBIEDs @ 100 KG each	Sufficient booster charge for 4,000 KG of homemade explosives in VBIED
Explosive	**Pressure Equivalent**	**Impulse Equivalent**	**Maximum Pressure**
TNT	1.00	1.00	
C-4 Composition B (60 RDX/40 TNT)	1.30 1.20	1.50 1.10	
Pentoxide Dynamite 60 % straight -50 percent -20 percent	1.42 0.90 0.90 0.70	1.44 0.90 — —	
Blasting gel ANFO	0.85 0.82	0.85	
Smokeless powder (dense pack) Black powder (dense pack)	0.60 0.60		
Photo flash powder (aluminum, potassium perchlorate 40/60)	0.42		
Fuel-Air (by weight)			
Ethylene oxide MAPP (welding gas)	10+ 10		300 PSI 200 PSI
Acetylene Propane	6		150 PSI 120 PSI
Methane Paint pigments			100 PSI 160 PSI
Milk powder Flour	7		135 PSI 150 PSI
Wood Sugar	7		160 PSI 134 PSI
Aluminum	10		195 PSI

Source: DHS

3. Effective Blast-Protection Measures

While it is not possible to fully protect passengers and facilities from an explosive attack, there are measures that can be put in place that can either reduce the potential for an attack or reduce the effectiveness of such an attack. In addition, the most effective security programs use multiple protective measures to enhance the overall results. Many of the protection measures mentioned in this section require some level of integration with the structural design or layout of the airport. Therefore, careful consideration will need to be taken early to ensure that implementation of these measures does not result in downstream consequences creating a more hazardous situation or impede operations.

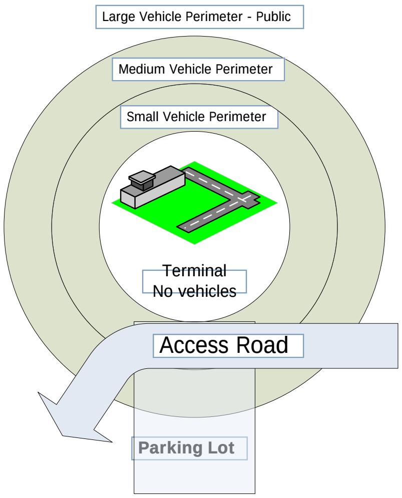
a. Blast-Protection Protocols

- Blast Envelope

Typical security protocols involve the establishment of security perimeters, or rings, that act as filters to keep potential threats from their targets. In this case, during higher threat potential, vehicle restriction would be imposed by the TSA to keep VBIEDs from the terminal. This system of rings can manifest itself in many ways. A blast analysis should be performed to identify the terminal's blast envelope. This in turn will serve to identify the closest approach point to the terminal for specific size vehicles. Studies done by the Bureau of Alcohol, Tobacco, and Firearms and Explosives (BATF) have identified some basic vehicle sizes and explosive carrying capacities, as shown in Table B-2.

By basing blast analyses on these carrying capacities, an airport can have graduated blast envelopes that allow certain size vehicles closer to critical infrastructure. Therefore, in cases of higher threat levels, vehicles would be restricted to areas outside their respective blast envelope (refer to Figure B-9).

Figure B-9. Blast Envelope



Source: TranSecure, Inc.

- Vehicle Inspections

One extreme measure is to not allow any traffic near the terminal during higher threat levels. However, other measures use the inspection of vehicles as a means of minimizing a VBIED attack. The goal is for airport personnel conducting the inspections to identify large items located in the trunk or bulk cargo areas of a vehicle that may house explosives.

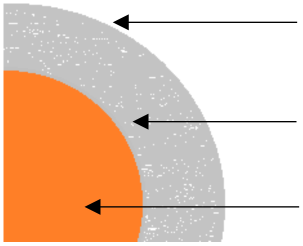
Vehicle inspections should be conducted away from the airport's critical infrastructure, and in a location where vehicle congestion will have minimal effect on the local community. It is often good to have inspection points placed in a manner that allow vehicles to turn around or away from the inspection point, since some of the larger vehicles (e.g., construction trucks) may not be possible to inspect. It is important that these alternative routes do not lead to the terminal; they are not to be considered as bypass routes, but as routes to lead vehicles away from the inspection area, perhaps into a remote parking area instead. Care should be taken to ensure that any potential alternative route is securely blocked so that uninspected vehicles cannot gain access to the terminal or other critical infrastructure.

Table B-2. Examples of Various Explosives Capacities

Bomb Threat Stand-Off Distances

This table is for general emergency planning only. A given building's vulnerability to an explosion depends on its construction and composition. The data in these tables may not accurately reflect these variables. Some risk will remain for any persons closer than the Outdoor Evacuation Distance.

	Explosives Capacity[1] (TNT Equivalent)	Mandatory Evacuation Distance[2]	Preferred Evacuation Distance[3]
 Pipe bomb	5 LBs 2.3 KG	70 FT 21 M	1,200 FT 388 M
 Suicide vest	20 LBs 9.2 KG	110 FT 34 M	1,750 FT 518 M
 Briefcase/suitcase bomb	50 LBs 23 KG	150 FT 46 M	1,850 FT 580 M
 Sedan	500 LBs 227 KG	320 FT 98 M	1,950 FT 580 M
 SUV/van	1,000 LBs 454 KG	400 FT 122 M	2,400 FT 732 M
 Small delivery truck	4,000 LBs 1,814 KG	640 FT 195 M	3,800 FT 1,159 M
 Container/tanker truck	10,000 LBs 4,538 KG	880 FT 263 M	5,100 FT 1,555
 Semi-trailer	60,000LBs 27,216 KG	1,570 FT 479 M	9,300 FT 2,835 M



Preferred Evacuation Distance
Preferred area (beyond this line) for evacuation of people in buildings and mandatory for people outdoors

Shelter-In-Place Zone
All personnel in this area should seek shelter inside a building away from the windows and exterior walls. Avoid having anyone outside – including those evacuating – in this area.[4]

Mandatory Evacuation Distance
All personnel must evacuate (both inside and outside of buildings)

[1] Based on maximum volume or weight of explosive (TNT equivalent) that reasonably fit in a suitcase or vehicle

[2] Governed by the ability of typical US commercial construction to resist severe damage or collapse following a blast. Performances can vary significantly, and buildings should be analyzed by qualified parties when possible.

[3] Governed by the greater of fragment throw distance or glass breakage/falling glass hazard distance. Note that pipe and briefcase bombs assume cased charges that throw fragments farther than vehicle bombs.

[4] A known terrorist tactic is to attract bystanders to windows, doorways or outside with gunfire, small bombs or other methods and then detonate a larger, more destructive device, significantly increasing human casualties.

Source: DHS

- Mobile Patrols

  In addition to physical enhancements, mobile patrols can provide a significant deterrent, especially when they are coupled with canine patrols. Patrols can monitor curbside vehicle activity to spot any unusual driving behavior, as well as passengers and personnel inside the terminal. Canine patrols can be used throughout the airport environment as a means to detect (not to clear out) possible explosive devices or vehicles. Once an IED is suspected, only the responding bomb squad can actually clear the device or determine its safety.

b. Physical Hardening Methods

As noted above, airports often have many vulnerable areas, facilities, and components. The following is a brief overview of methods and materials that can be employed to physically protect and harden the airport and its various components. In addition, some limitations of these hardening techniques also are listed.

- Window Films

  Many window film systems for the hardening of existing windows have been developed and blast tested. These window films, when properly installed in a suitable window frame, will resist small IED blasts.

  Limitations: When the design blast pressure is exceeded, large “panels” of the hardened windows tend to fail. A secondary “catcher” system behind the windows may also be needed. Window films offer no ballistic resistance. The aesthetics of the window hardening film should be considered. Some of the film systems require a thick bead of caulking at the window edges. Other systems require extensive window frame reinforcing. A mock-up of an in-situ window panel should be performed prior to implementing this material.

- Conventional Window Replacement

  Current “state-of-the-art” window replacement systems can resist peak blast pressures of approximately 10 to 20 pounds per square inch (psi). Blast-resistant window systems should be laminated and/or thermally treated glass. A catcher system can be installed behind the windows to augment the performance of laminated glass systems. Replacement windows can also provide ballistic protection if required.

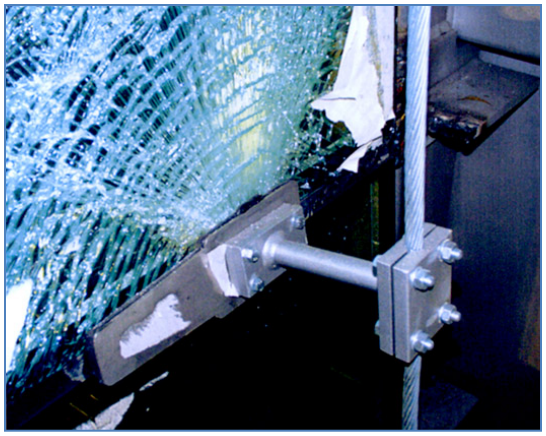
  Limitations: Very few full-scale blast tests of replacement window systems have been performed. Most tests have been performed on small window panels in rigid window frames. This testing may not accurately reflect actual in-situ conditions for large curtain walls. Blast-resistant glazing requires special detailing and design.

- High-Energy Absorbing Window Systems

  Blast analysis and some testing have been performed on curtain wall systems that absorb blast energy rather than trying to reflect it. The analysis shows that very high blast pressures can be absorbed. By absorbing the blast energy, the effective pressure on the glazed panels is reduced significantly. Thus, the windows can be thinner and less costly. High-energy absorbing window systems can replace existing curtain walls or be installed behind existing glass and doorways to provide transparent blast protection.

  The fractured glazing image (Figure B-10) shows a successful blast test of a “high energy-absorbing cable-supported curtain wall glazing system.”

Figure B-10. High Energy-Absorbing Cable-Supported Curtain Wall Glazing System



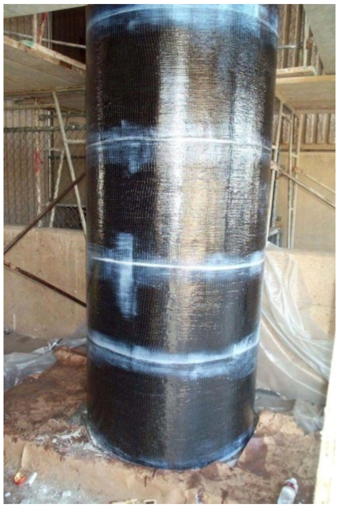
Source B-10/11: Magnusson Klemencic

Table B-3. Blast Resistant Window Criteria

Performance Condition	Protection Level	Hazard Level	Glazing System Response
1	Safe	None	Glazing does not break. No visible damage to glazing or frame.
2	Very high	None	Glazing cracks but is retained by the frame. Dusting or very small fragments near sill or on floor acceptable.
3a	High	Very low	Glazing cracks. Fragments enter space and land on floor no further than 3.3 ft. from the window.
3b	High	Low	Glazing cracks. Fragments enter space and land on floor no further than 10 ft. from the window.
4	Medium	Medium	Glazing cracks. Fragments enter space and land on floor and impact a vertical panel at a distance of no more than 10 ft. from the window at a height no greater than 2 ft. above the floor.
5	Low	High	Glazing cracks and window systems fails catastrophically. Fragments enter space impacting a vertical panel at a distance of no more than 10 ft. from the window at a height greater than 2 ft. above the floor.

Source: GSA Test Protocol GSA-TS01-2003

Figure B-11. Column Wrapping Procedure



Source: Karagozian-Case

- Column Wrap

  Kevlar and carbon fiber wraps (refer to Figure B-11) can substantially improve the blast resistance of reinforced concrete columns. These systems have been installed in several retrofit conditions. Limitation: The column wrap will cover the visual surface finish and texture of the columns.

  Column Steel Jackets can substantially improve the blast resistance of reinforced concrete columns. These systems have been installed in several retrofit conditions.

- Polyurethane/Polyurea Elastomer Coating

  Walls constructed of 2x4 wooden studs and clad with particleboard and aluminum siding have been successfully blast tested. CMU walls have been coated with polyurea coating and blast tested as well. This coating may need to be fireproofed for certain applications.

- Composite Wall of Steel-Plated Walls

  Testing and analysis has shown that a composite wall system (Figure B-12) can provide blast and ballistic protection from VBIED size bombs at close proximity. Corner columns cannot be protected in this manner, and this system does not prevent slab or girder breaches from explosions.

- Catenary Cable Floor Support System (Missing Column Strategy)

  Analysis and tests to date prove that catenary cables effectively prevent progressive collapse due to a “missing column” (Figure B-13).

Figure B-12. Composite Wall of Steel Plated Walls

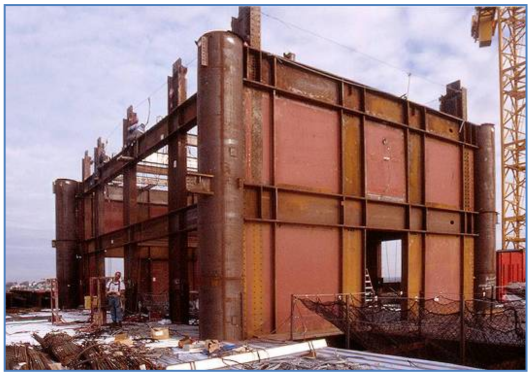
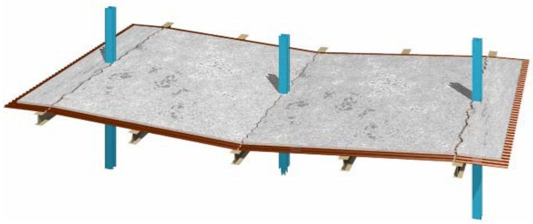


Figure B-13. Catenary Cable Floor Support System



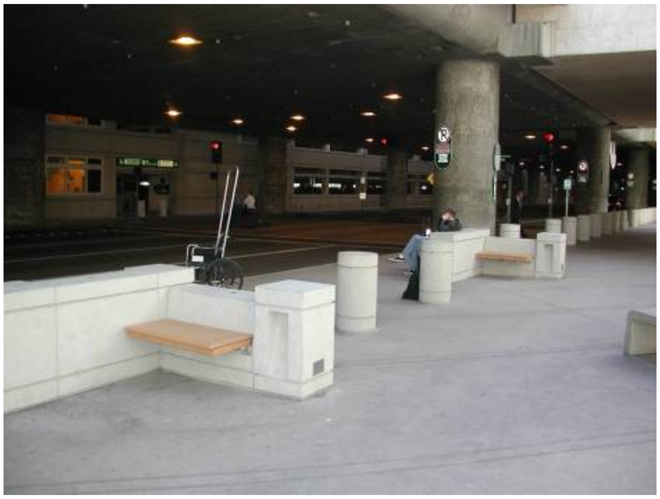
Source: for B-12, 13 & 14, Magnusson Klemencic Associates

- Vehicle Barriers

  Vehicle barriers can effectively protect facilities and columns from vehicular impact and bomb blasts by creating standoff between the target and the threat. The barriers can be designed for a variety of vehicle sizes. Barriers can be installed in both at-grade conditions (refer to Figure B-15) and elevated structures.

Limitations: Aesthetic and operational issues should be considered prior to deploying vehicle barriers. Operational issues resulting from narrowed roadways, including fire truck and emergency vehicle access, should be considered prior to erecting vehicle barriers.

Figure B-14. Vehicle Barrier—at Grade



- Threat Containment Room or Area

Blast tests have shown that small IEDs can severely damage large-diameter reinforced concrete or steel columns. Furthermore, this size of explosive would cause many casualties. Thus, it is extremely important that "suspicious" items be addressed rapidly and effectively. Consideration should be given toward the provision of an accessible and convenient blast-hardened room or blast-hardened outside area in or near the terminal that is robust enough to safely contain a blast from a small IED that would fit in a suitcase. In addition, the hardened room will need to be vented outside and perhaps have a dedicated ventilation system to control chemical or biological contamination. Proprietary threat containment vessels also should be considered (refer to Figures B-15 and Figure B-16). Another option is to use dual-plate composite blast walls for this protection.

- Threat Containment Vessel

Proprietary Threat Containment Vessels (TCV) are available to resist IEDs of various sizes. A vessel capable of resisting a 50 pound TNT charge would suit most airport applications (Figure B-15). Some models can contain chemical and biological gasses as well.

Figure B-15. Large IED Threat Containment Vessel

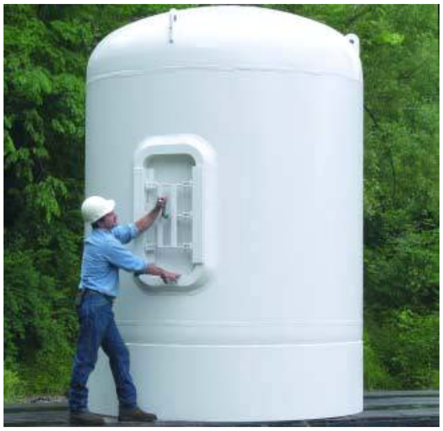
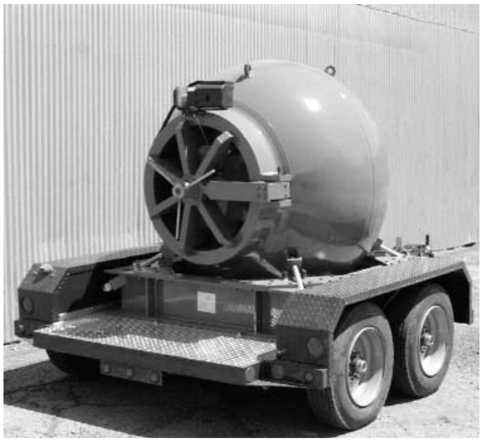


Figure B-16. Small IED Threat Containment Vessel



Source B-14, 15, & 16: Karagozian & Case

A mobile Threat Containment Unit (TCU; Figure B-16) is capable of providing safe storage of small IEDs (7 pounds of TNT).

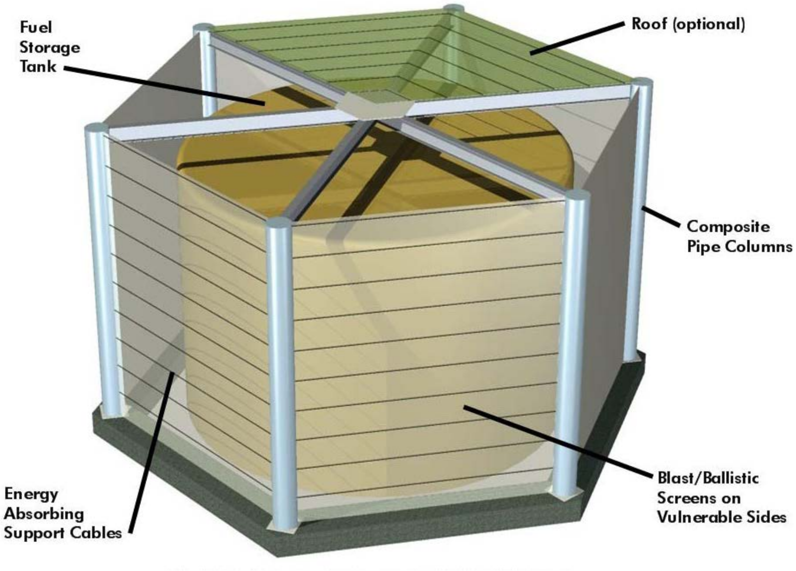
Limitation: The portable TCU cannot contain chemical and biological agents when dispersed with explosives.

- Fuel Storage Tank Protective Screen

  To protect fuel tanks, substations, and related equipment, a blast/ballistic screen assembly (refer to Figure B-17) can be installed to shield this equipment from most car bombs and high-powered rifle attacks. The screen material would likely be Kevlar or ornamental plate steel, depending on the threat. The screens are hung from energy absorbing steel cables that dampen the blast energy tremendously. The columns that support the screens likely would be constructed of steel pipes filled with concrete (composite columns), which have excellent blast-resistance and strength properties.

  When constructing new fuel tanks for aircraft or rental cars at airports, consider buried tanks or recessing the tanks in a pit such that the tanks are not visible above grade and difficult to target with small arms. Also, when the tanks are recessed below grade, the surrounding soil helps mitigate the resulting blast if they are detonated.

Figure B-17. Blast and Ballistic Screen Assembly for Fuel Storage Tanks


Fuel Storage Tank
Roof (optional)
Composite Pipe Columns
Blast/Ballistic Screens on Vulnerable Sides
Energy Absorbing Support Cables

Source: Kargozian & Case

- Baggage Inspection Room

  Baggage screening rooms offer little protection to the surrounding terminal facility, passengers, TSA baggage inspectors, or the police bomb squad contacted to assess and de-fuse a suspect IED. Current TSA protocol dictates that suspicious bags identified by in-line baggage screening devices are tagged for secondary “visual” inspection. Subsequently the suspect bag is redirected to the bag inspection room for a visual inspection by opening the suspect bag and observing the contents. Opening the suspect bag might inadvertently detonate an IED or the bag itself may have a detonation trigger. If an IED is discovered, the TSA is directed to immediately leave the area, notify the bomb squad, and evacuate all or a portion of the airport terminal building.

  Items to consider for improving the safety and operations of the baggage inspection room include the following:

  a) Perform drills at all bag screening rooms to observe the action of the TSA and bomb squad if an IED is discovered while opening a bag. The “Threat Containment Unit” (TCU) access and response time would be evaluated and improved as needed. Also the communication protocol will be observed and clarified or modified if needed.

b) Consider placing an explosive disposal container capable of resisting a five to seven pound IED within or near the baggage screening room. A blast resistant trash container, for example, could be used for this. The bomb squad may elect to place the IED in this container prior to disarming or transporting the device out of the terminal building.

c) Consider hardening the bag inspection room. There are a variety of blast resistant, cost-effective wall, window, column, and ceiling system measures that can readily harden the room. For example, a wall and ceiling constructed of metal panels with the cavity filled with sand is very cost-effective and able to effectively mitigate small IED devices. A blast resistant skin can be added (retrofitted) to the existing walls to help mitigate an IED.

d) Evaluate and move critical services, utilities, and distribution systems away from the bag screening rooms.

e) Provide a wash station and shower in or near the bag screening room so that TSA personnel or the bomb squad can shower and wash off potential chemical and biological agents.

f) Provide a tightly sealed room and doors with a dedicated ventilation and filtration system so that chemical/biological agents can be contained.

g) If possible, move the bag screening rooms to locations that are accessible to the outside and can vent blast pressures outward.

4. Blast Analysis Tools

Many blast analysis tools are available to evaluate and predict the effects of blasts on a building structure. It is important that the engineers using these tools understand the proper use and limitations of this software. Access to blast analysis programs is usually limited, and engineers must be authorized in order to obtain these security-sensitive programs.

The level of detail presented and used in a blast analysis can vary to extremes. Desired level of detail is a direct function of cost—extremely detailed analyses can be very expensive, while simpler and less expensive ones may be sufficient for the facilities being evaluated.

Engineers should evaluate the propensity of their structures to succumbing to progressive collapse. This is an important aspect of any good blast analysis. The removal of a key load-bearing structural member may propagate the failure of other key structural components throughout the facility. The consequences of such a failure are obvious. Such an attack achieves the desired result not by blast force and fragmentation, but by structural failure. Many of the blast analysis software programs available do not take into consideration the transfer of the dead loads of the missing structural member to other surrounding members and their subsequent ability to support those additional loads. This type of evaluation is usually performed separately from the blast pressure load calculations.

Guidance for conducting blast analyses can be found in the Federal Emergency Management Agency’s Manual 426, *Risk Management Series: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings.* Appendix A of this document discusses different methods by which designers can assess potential damage to their facilities.

APPENDIX C: International Aviation Security

The fastest growing segment of air travel is international flights coming to the United States. FAA forecasts cite a 2.0% growth rate for domestic passengers, on average, through 2036. International passengers to the United States are forecast to grow at a much higher rate – an average of 3.8% per annum over the next 20 years[14].

At the same time, the recommended guidelines for facility security are influenced by several areas in recent years:

- Changes to handling of checked bags
- Expansion of US Preclearance
- Role of other government agencies to help with clearances

1. Planning Requirements

US Customs and Border Protection 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.

a. CBP Mission Requirements

In accordance with CBP's mission to secure the nation's borders while facilitating trade and travel, CBP processes and controls U.S.-inbound 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 uses a number of technologies and processes to facilitate passenger processing, and will provide the airport operator with information on technologies as they impact design and construction processes. CBP also facilitates the work of other government agencies, including the CDC, among others, in the clearance of goods and people.

b. Role of Airport Technical Design Standard

CBP's *Airport Technical Design Standard* was last published in 2011 and is expected to have an updated version in 2017. The facility includes specifications for size of facility based on the number of peak hour inbound passengers, as well as requirements for security and process flows for passengers/checked bags.

c. Recent Process Changes

CBP is undertaking a major "Business Transformation" effort to reduce the amount of manual work for CBP officers and increase the potential of automation and partnerships with airlines/airports. Some results of CBP's Business Transformation Initiatives[15] include:

- Deployment of Automated Passport Control kiosks to reduce wait-time for CBP processing
- Implementation of Mobile Passport Control to enable eligible passengers with a smartphone to answer questions in-flight before landing

[14] https://www.faa.gov/data_research/aviation/aerospace_forecasts/

[15] https://www.cbp.gov/newsroom/speeches-and-statements/2016-03-16-000000/commissioner-kerlikowske%E2%80%99s-remarks-congressional for a more detailed review of CBP Business Transformation

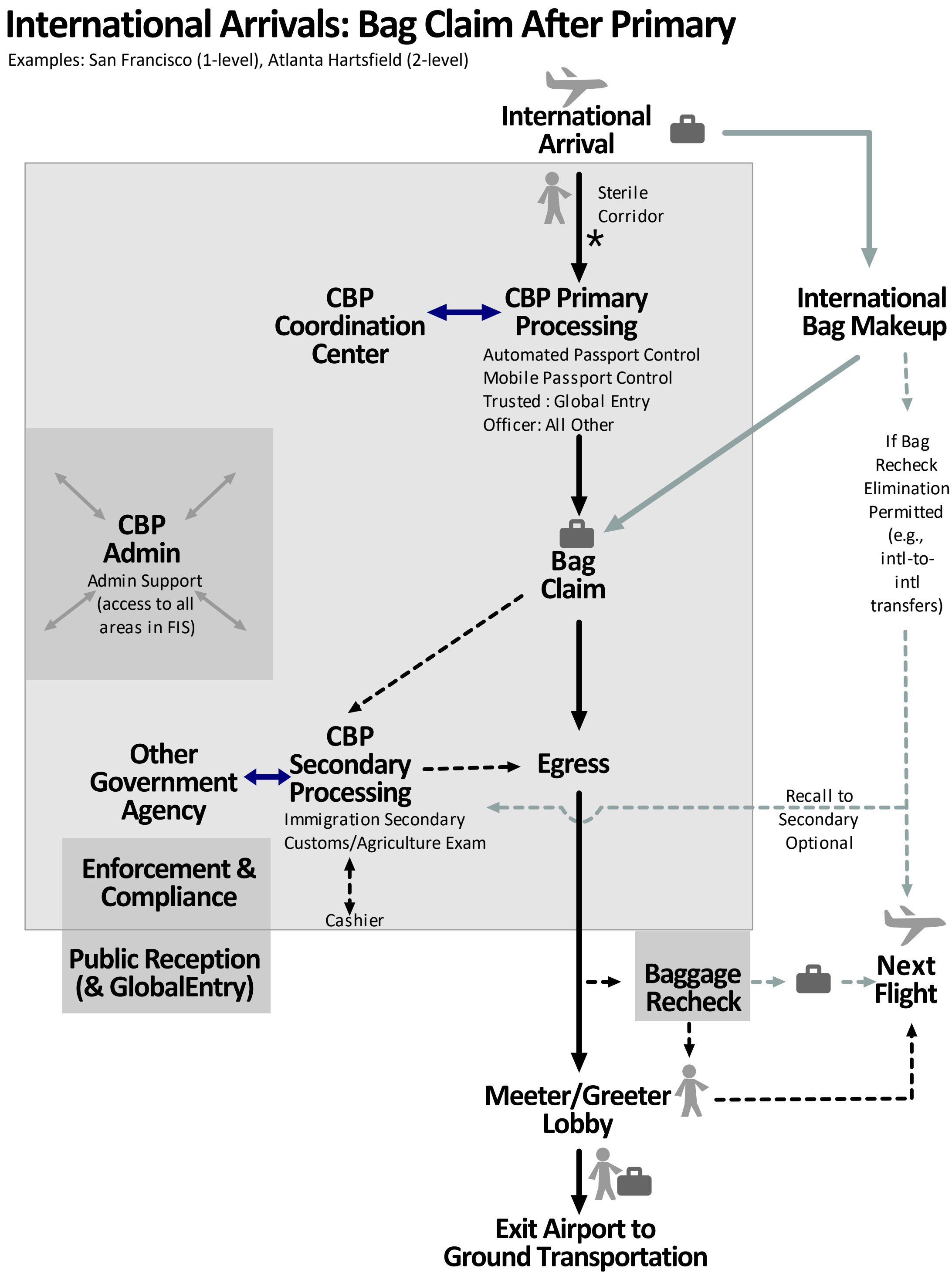
- Expansion of Global Entry, with full access to TSA Pre✓™ lanes

Additional changes with impacts on facilities include:

- Baggage recheck elimination for certain connecting flights (e.g., IAH, DTW)
- Implementation of inbound screening processes (e.g., Ebola)
- Deployment of “Baggage First” at select airports (e.g., AUS)

In addition to the facility changes, extraordinary screening measures were instituted during the Ebola outbreak of 2014–15. While the CDC advocated for pre-departure screening in affected source countries for Ebola, in October 2014 CBP began a process for screening passengers at major inbound gateways and referring cases to CDC for interdiction on arrival. These temporary measures were only in place at one of five U.S. airports conducting enhanced entry screening (JFK, IAD, EWR, ORD, and ATL), and were stopped in late 2015.

Figure C-1. International Arrivals: Bag Claim after Primary



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

Source: InterVistas

For regular operations at most CBP facilities, passenger flows are similar to the 2011 set of processes. As shown in the following diagram, an international arrival proceeds to CBP primary processing. Now there are a range of automated solutions (e.g., Automated Passport Control, Global Entry) 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. At airports such as IAH, ATL, and DTW, there is no need for a baggage recheck. In this case the diagram on the previous page 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.

2. Major Facility Changes

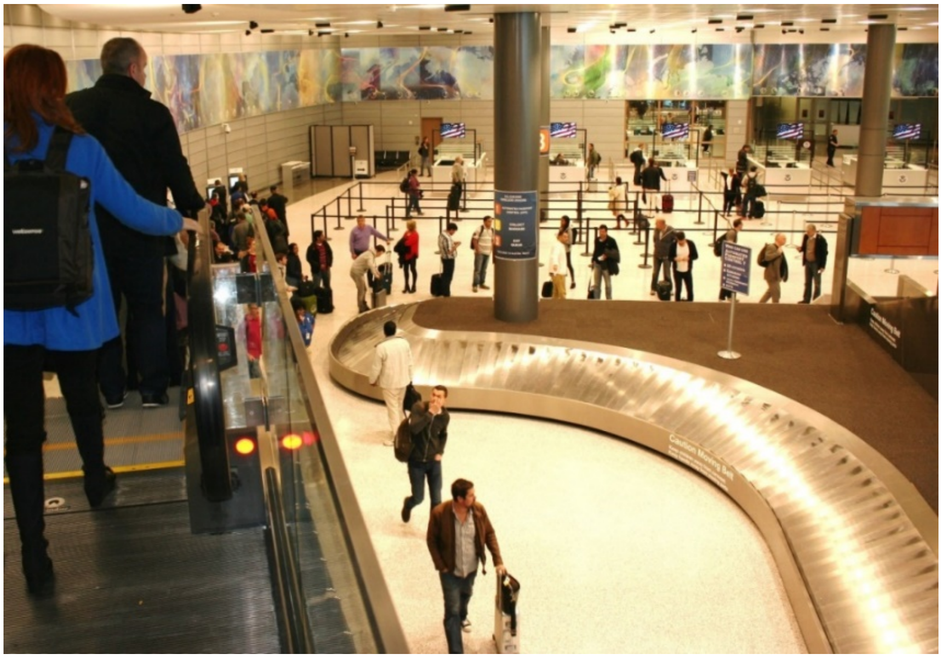
a. Bags First

Legacy agencies (Customs, Immigration & Naturalization Service) created a “primary” and “secondary” processing in 1971 to address volumes. Most facilities built subsequent to this time were created to allow bag claim after primary processing (passport check, biometric for foreign nationals, declaration).

The *Airport Technical Design Standard*, over the past 20 years, has held to the separation of functions for “primary” and “secondary.”

Changes are advanced for CBP to allow “Bags First”, also known as “one-stop.” Under this process, all passengers pick up bags first, before proceeding to see a CBP officer.

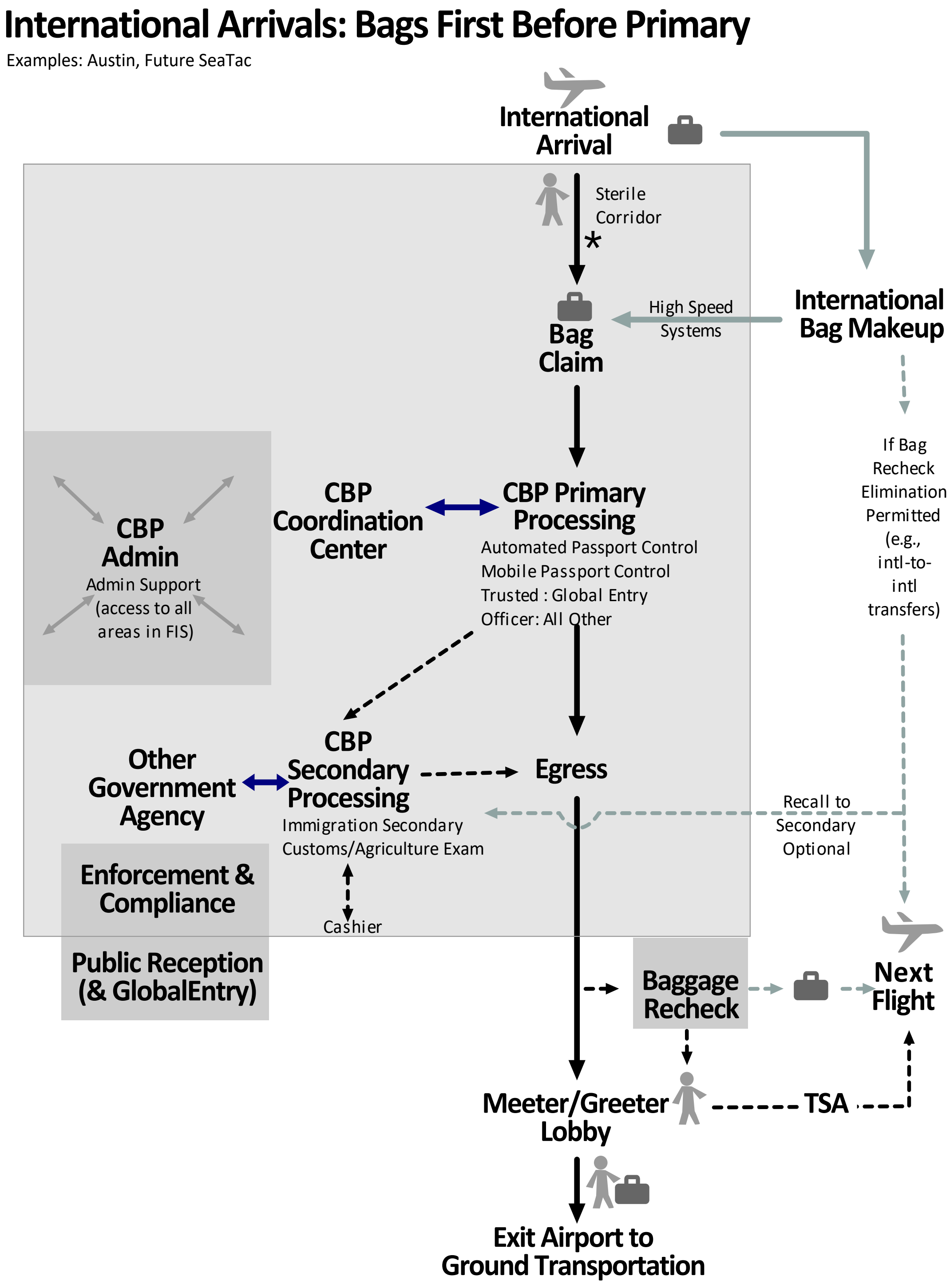
Figure C-2. Bag Claim before CBP at AUS



Source: InterVistas

There are implications for the baggage security with the changes in flows for bags, and their proximity to recheck/re-screening devices. The optional process flows are shown in the following flow diagram:

Figure C-3. International Arrivals Bags First before Primary



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

Source: InterVistas

The new facility flows will also be advanced at SEA in 2019, as well as other new CBP facilities planned in future.

3. Preclearance Expansion

CBP processes some 112 million passengers a year. In 2016, there are 15 pre-clearance sites around the world performing full CBP clearances in Canada, Caribbean, Ireland and Abu Dhabi. In 2015, 11 new sites were announced for consideration, including Amsterdam Schiphol, Punta Canada, Stockholm, Manchester, Tokyo Narita, among others.

CBP has a stated goal to reach 33% of passengers pre-cleared by 2025 – up from some 15% today. There are several facility impacts that have implications for US airports and CBP facilities. They include:

a. Elimination of TSA re-screening for precleared passengers and bags, provided TSA standards for screening are met. Similar to arrangements from pre-cleared airports in Canada, if equipment and processes are deemed equivalent, there is no need for TSA re-screening for passengers connecting to an onward international or domestic US flight.

b. Shared baggage facilities: most domestic US airports are not planned for large amounts of wide body gates. New preclearance flights could prompt the demand for large aircraft (e.g. A380) 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.

As a result, the design of CBP facilities are expected to be increasingly shared between domestic and international operations, with associated physical planning and operational security measures needed to prevent co-mingling of cleared/uncleared passengers. In addition to the 11 potential new sites, CBP 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.

4. International Aviation Security Checklist

- □ Model the proposed design to ensure clear and unambiguous passenger flow
- □ Model various processing times and passenger flows through exit control
- □ Life safety issues vs. security requirements have equal footing
- □ Establish a task force to review design parameters, document changes, and agreements
- □ Changes will occur; establish protocols for review of changes
- □ Coordinate w/ FIS Security Plan
  - ▪ Contact CBP; Federal Agencies
    - ▸ Obtain CBP *Airport Technical Design Standards*
    - ▸ Obtain Workforce Analysis Model (WAM).
  - ▪ Address Issues in FIS Plan
    - ▸ Physical Safeguards
    - ▸ Plans/Procedures for Implementation
    - ▸ Resources to Sustain FIS Protection Program
  - ▪ Coordinate FIS Security Requirements with Airport ConOps and ASP
    - ▸ Access Control
    - ▸ CCTV
    - ▸ Baggage Screening and EDS
    - ▸ Perimeter Protection
    - ▸ IT Systems, Video, Voice, and Data Networking
- □ FIS Design, Construction, Acceptance, and Occupancy
  - ▪ Provide for CBP/Agency Involvement in Specifications, Drawings, and Construction Documents
  - ▪ Schematic Design
    - ▸ Model variability in processing times using the CBP Model
      - • Architectural, Security and IT Integration
    - ▸ Construction Bid Package
    - ▸ CBP written approval at each step
    - ▸ Establish change review process

APPENDIX D: General Aviation

Recommendations in this section are tailored for general aviation (GA) operating areas located at airports with commercial (scheduled passenger airline) service and regulated under CFR § 1542. Commercial service airports, as well as airports serving only GA aircraft, can find additional information specific to GA in *TSA's 2004 Security Guidelines for General Aviation Airports*. The GA Subcommittee of TSA's Aviation Security Advisory Committee has drafted updates that have not been approved for release as of this writing. However, many of the airport security concepts put forth in the preceding sections of this Guidelines document can easily be adapted and scaled to meet GA airport needs.

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).

1. 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 U.S. air traffic. GA operations are typically asymmetric, and 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 a GA 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 general aviation may result in unnecessary restrictions, potentially causing a decline in operations at the airport and a drop in GA activity and revenues.

2. Security Areas and Boundaries

As discussed in Section 5, Airside, it is advisable to exclude GA operating areas from the SIDA of the airport as much as is practicable. In the event this is not possible, operational limits should be considered to eliminate any possible breach of § 1542 security. 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.

a. At commercial service airports where the Aircraft Operating Area (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 an unnecessary security response.

b. 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.

c. Separation is normally accomplished by designing GA parking areas that lie outside of areas secured for commercial operations, often on the opposite side of the airport.

d. Design ramp parking arrangements to ensure visual observation of aircraft and passengers during the embarking and disembarking process.

Preclearance procedures for airport GA facilities are set forth in *CBP Preclearance of General Aviation Summary Guide*, Version 3, March 2014, U.S. Customs and Border Protection of DHS.

3. Ramp Security Measures

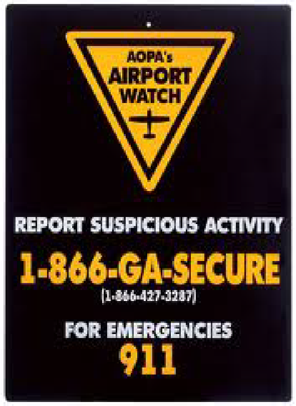
Fixed-Base Operators (FBO)/GA terminal operators should consider the design of secure or monitored access doors and gates for each portal leading to the aircraft ramp. They should provide signage that clearly restricts access to the AOA to authorized persons only. Depending on individual airport security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

4. 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, i.e., AOPA's Airport Watch 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, whichever is appropriate (see Figure D-1).

Figure D-1. AOPA Airport Watch Sign



Source: AOPA

5. Lighting and Cameras

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

a. Aircraft parking and hangar areas

b. Fuel storage areas and fuel trucks

c. Airport access control points, including perimeter

d. Other appropriate areas, such as vehicle parking, fences or obstructed areas

6. 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 to airport through pedestrian gates or key code access, when appropriate. Depending on airport security requirements and AOA configuration, airport ID badging might be required.

7. Building Design Factors

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

a. The Customer Service Representative Reception area should have a clear view of all doorways and other access points leading to the ramp.

b. 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 access control and alarm monitoring system. Ramp access from the FBO or terminal should be controlled and restricted to authorized personnel only.

c. 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.

d. Planners should consider minimizing ramp access by all vehicles as much as possible.

8. International General Aviation

Where possible, the design of separate CBP or Federal Inspection Areas should be incorporated using the design standards for a general aviation Federal Inspection Services (FIS) facility (Chapter 8, “General Aviation Facilities,” of the Customs and Border Protection document, *Airport Technical Design Standards*). National Safe Skies Alliance has also undertaken a project to provide updated guidance to airports for FIS facilities, which is not yet completed at this writing.

AUTHOR ACKNOWLEDGMENTS

CONTRACT STAFF

TranSecure Inc.

Art Kosatka	Project Manager and Principal Investigator
James McGuire	Technical Director – Video, IT, Communications
Kristina Dores	Subject Matter Expert – Airport Operations
Quinten Johnson	Subject Matter Expert – Aviation Security Operations/Management
Nancy Hill Ward	Project Administrator/Co-editor

Arts & Engineering PLLC

Hunter Fulghum	Subject Matter Expert – Engineering

Vesper Hill Research & Analysis

Courtney Tucker	Subject Matter Expert – Security, Legislation Regulations

Magnusson Klemencic

Terry Palmer	Subject Matter Expert – Blast Protection/Mitigation

InterVistas

Solomon Wong	Subject Matter Expert – International FIS Facilities

Crowznest Consulting

Don Zoufal	Subject Matter Expert – Safety, Operations, Integration

SDI Inc.

Tom Condon	Subject Matter Expert – Safety, Security, Human Factors

CONTRIBUTORS

The principal contractor, TranSecure, Inc., could not provide such a wide range of information without the extensive assistance and input from a broad array of industry and government subject matter experts contacted for this updated guidelines document. This includes both executives and security practitioners from the principal trade associations, regulatory agencies, labor unions, architect and engineering firms, consultants, and airports, including:

Transportation Security Administration
Federal Aviation Administration
Department of Homeland Security
Airport Consultants Council Security Committee
Airports Council International – North America Security Committee
American Association of Airport Executives Security Committee
Aircraft Owners and Pilots Association
Airlines for America
Airline Pilots Association
Particular thanks go to following individuals who contributed:

Contributor		Affiliation
Thomas	Anthony	Univ. Southern California
Marc	Beningson	Parsons Brinckerhoff
Alan	Black	DFW Airport
Jonathan	Branker	FAA
Nina	Brooks	ICAO
Jose	Chavez	TSA
Charles	Cinquemani	DFW Airport
Roger	Cotterill	TSA
Ron	Crain	Burns & McDonnell
Kristi	Crase	Quantum Secure
Michael	Duffy	TSA
Dan	Flynn	Security Radar Integrators
Keith	Goll	TSA
Neville	Hay	Gatwick Airport
Robert	Hope	Burns & McDonnell
Tim	Hudson	Gensler
Amber	Kasbeer	TSA
Michael	Keegan	Milwaukee Airport
Ed	Kittel	TSA
Warren	Kroeppel	Sheltair
Enrique	Melendez	Leidos
Lance	Nuckolls	FAA
Jeanne	Olivier	PANYNJ
Michael	Pilgrim	Burns & McDonnell
David	Pollard	Tallahassee Airport
Susan	Prediger	SP Consulting
James	Prokop	TSA
Charles	Reed	Parsons Brinckerhoff
Jay	Romlein	CSHQA
Nobuyo	Sakata	AOPA
Mark	Schuettte	Burns & McDonnell
Lon	Siro	TSA
Joseph	Smith	Applied Research Assoc.
Craig	Spence	AOPA
David	Stewart	IATA
Lars	Suneborn	Smart Card Alliance
Fred	Terry	Burns & McDonnell
Tony	Thompson	BetaFence USA
Christer	Wilkinson	AECOM
Payton	Warner	American University
Leonard	Wood	Condor Aviation