Recommended Security Guidelines for Airport Planning, Design and Construction

Revised June 15, 2006

Transportation Security Administration

THIS PAGE INTENTIONALLY LEFT BLANK

NOTICE

This document is distributed under the sponsorship of the Transportation Security Administration of the U.S. Department of Homeland Security in the interest of information exchange. The U.S. Government assumes no liability for the contents or use.

This document does not create regulatory requirements. There are recommendations and guidelines contained in this document that might be considered highly beneficial in one airport environment while being virtually impossible to implement at another airport. The purpose of the document is to provide as extensive a list of options, ideas, and suggestions as possible for the airport architect, designer, planner and engineer to choose from when first considering security requirements in the early planning and design of new or renovated airport facilities.

This document provides numerous references to and citations from other government and industry sources. These are not intended to be modified by this document in any way, and are generally intended to refer to the most current version of such external resources, to which the reader should go for detailed information.

This document may be downloaded free of charge from the following TSA Internet site: *http://www.tsa.gov*

Or contact the security coordinator at:

Airport Consultants Council (ACC):	703-683-5900
Airports Council International – North America (ACI-NA):	202-293-8500
American Association of Airport Executives (AAAE):	703-824-0500

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

This document is intended to bring to the attention of the airport planning, design, and engineering community the serious security concerns that must be considered for incorporation into an airport design at the earliest possible planning stage, in order to bring the most efficient and cost-effective security solutions to bear. An undertaking as extensive and comprehensive as this requires the participation and cooperation of a wide range of aviation security professionals contributing time, experience, knowledge and insight. We hope that this document accurately captures the experiences of the past and will help the reader anticipate the needs of the future.

To complete the current revision of this document, an Aviation Security Advisory Committee (ASAC) Working Group was formed. Under the auspices of this working group, over 100 persons attended meetings and participated in document reviews. A few participants, referred to as Section Chiefs, supervised edits of specific sections of the document. These and other participants rewrote outdated material, edited drafts, and brought current practices, real-world perspectives and new federal regulations to the table, advising the Working Group of what would, and would not, work in an operating airport environment.

This document is not intended to be the final word on airport security design; it is meant to be a primer on the security issues important to airport development and a check-list of the more important things one must consider when deciding which of the many potential security approaches may be appropriate to a particular airport's circumstances and requirements.

We wish to acknowledge the invaluable contribution of all the participating organizations and persons listed below. Special thanks also go to:

Mike Duffy with the Transportation Security Administration (TSA), who proposed creation of the working group and supported this project from start to finish;

Joe Corrao with the TSA who served as the Working Group Executive Director;

Joe Kris and Scott Foulger with the TSA who served at various times as the TSA Working Group Co-Chairs;

Paula Hochstetler with the Airport Consultants Council (ACC) who served as the industry Working Group Co-Chair;

Suzanne Guzik with CTI Consulting who helped assemble and edit the revised draft document;

Bob Mattingly with Sarasota Bradenton International Airport, who attended every meeting and made significant technical contributions to the entire document; and to

The following individuals who served as Section or Appendix Chiefs:

Airport Layout & Boundaries - Ken Cox with CTI Consulting

Airside – Ian Redhead with ACI-NA

Landside - Kenneth Hutton with the Metropolitan Washington Airports Authority

Terminal - Art Kosatka with TranSecure

Passenger Screening - Scot Thaxton with the TSA

Baggage Screening - Mark Torbeck with the TSA

Cargo Screening - Pam Hamilton with the TSA

ACAMS - Christer Wilkinson with DMJM Technology

Video Surveillance, Detection & Distribution - James McGuire with MHR International, Inc.

Power, Communication & Cabling Infrastructure - Tom Coleman with DHS TSL & Rebecca Morrison with AAAE

International - James McGuire with MHR International, Inc.

Airport Blast Protection - Amber Kasbeer with DHS/TSA/TSL & Terry Palmer with Magnusson Klemencic Assoc., Inc.

Paula Hochstetler	Airport Consultants Council
Ian Redhead	Airports Council Int'l-NA
Dean Snyder	American Airlines
Rebecca Morrison	Amer. Assn of Airport Execs
Joe Erhart	Apple Designs, Inc.
Howard Burrows	Battelle
Mauricio Fernandez	Battelle
Susan Prediger	CAGE Inc.
Stephen Clarke	Carter & Burgess, Inc.
Terry Colegrove	Comm. Infrastructure Designs
Jim Willis	Convergent Strategies Consulting
Ken Cox	CTI Consulting
Suzanne Guzik	CTI Consulting
Bill Bruneau	Denver Int'l Airport
Armen DerHohannesian	DerHohannesian + Assoc., LLC
Jackson Stephens	DHS CBP
Dan Ziegelbauer	DHS CBP
William A. Fife	DMJM-Harris - NY
Christer Wilkinson	DMJM Technology
Jozef Grajek	EJG Aviation
Kelley Fredericks	Erie Municipal Airport Authority
Rick Marinelli	FAA
Steven Urlass	FAA
Michael Patrick	Gensler
Keith Thompson	Gensler
Marion Kromm White	Gensler
Mike Bolduc	Glover/Resnick & Assoc., Inc.
William Glover	Glover/Resnick & Assoc., Inc.
Ron Orchid	Glover/Resnick & Assoc., Inc.
Mitch Chokas	HKS, Inc.
Scott Hyde	Hartsfield Planning Collaborative
Theresa Coutu	InVision Technologies, Inc.
James Tucci	K&J Safety & Security Consulting
Michael DiGirolamo	Los Angeles World Airports
Robert Smallback	Lee County Port Auth.
Terry Palmer	Magnusson Klemencic Assoc.
Dennis Treece	MassPort Authority
Carl Scarbrough	McCarran Int'l Airport
Geoffrey Baskir	Metro. Washington Airports Auth.
Richard Cullerton	Metro. Washington Airports Auth.
Kenneth Hutton	Metro. Washington Airports Auth.
Jason Terreri	Metro. Washington Airports Auth.
James McGuire	MHR International, Inc.
Michael H. Ross	MHR International, Inc.
Mark Forare	Miami-Dade Aviation Dept.
Carolyn Strock	Mid-Ohio Valley Regional Airport
Fred Cummings	Philadelphia International Airport
Shane Shovestull	Phoenix Aviation Dept.
Jeanne Olivier	Port Authority of NY & NJ
Gorge Reis	Port Authority of NY & NJ
Cal Edmonson	Raleigh-Durham Int'l Airport
Bill Sandifer	Reynolds, Smith & Hills, Inc.
Craig Williams	Reynolds, Smith & Hills, Inc.
Mike Mini	Rhode Island Airport Corporation
Frances Sherertz	Sacramento County Apt System
Donna Edwards	Sandia National Labs
Bob Mattingly	Sarasota Bradenton Int'l Apt
Ted Kleiner	STV Incorporated
Art Kosatka	TranSecure
Gloria Bender	TransSolutions
Eric Miller	TransSolutions
Cenk Tunasar	TransSolutions
Anthony Cerino	TSA TSL
Tom Coleman	TSA TSL
Joe Corrao	TSA
Michael Duffy	TSA
Frederick P. Falcone	TSA
Brad Fawsett	TSA
Scott Foulger	TSA
Pam Hamilton	TSA
Amber Kasbeer	TSA TSL
David Kasminoff	TSA
Rigina Kim	TSA
Joseph Kris	TSA
Rick Lazarick	TSA TSL
Jordan Lerner	TSA
Scot Thaxton	TSA
Mark Torbeck	TSA
Kristina Dores	Unisys Corp
Michael Pilgrim	Unisys Corp
Archie Lind	URS Corporation
Mike Williams	Williams Gateway Airport
Franklin M. Sterling	Williams Sterling, Inc.
James Williams	Williams Sterling, Inc.

TABLE OF CONTENTS

PART III - RECOMMENDED GUIDELINES

PART IV - APPENDICES

FIGURES

TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

PART I

OVERVIEW

Section A - Introduction

This document presents recommendations for incorporating sound security considerations into the planning, design, construction, and modification of security-related airport facilities and airport terminal buildings. It consolidates information developed through the participation of the Transportation Security Administration (TSA) and other government and aviation industry professionals. The information in this document was gained through the experiences of a broad range of aviation security programs and projects at numerous United States (U.S.) airports, and through the continuing efforts of government and industry to develop improved approaches to incorporating cost-effective security features into the early planning and design of airport facilities. The information is presented here in a single document, which will be revised and updated periodically as regulations, security requirements, and technology change.

In response to the September 11, 2001 (9/11) terrorist attacks in the U.S., and with the potential for future attacks in this country, Congress passed and signed into law the *Aviation and Transportation Security Act (ATSA)*, Public Law 107-71, 115 Stat. 597 on November 19, 2001. The ATSA established the TSA as an operating administration within the Department of Transportation (DOT), headed by the Under Secretary of Transportation for Security.

Since that time, the Department of Homeland Security (DHS) 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 in over a half-century. To fulfill its mission, DHS identified several goals and objectives within its Strategic Plan; TSA supports these goals and objectives.

There are numerous advantages to incorporating security concerns into airport planning and design at the earliest phases. Timely consideration of such needs is almost guaranteed to result in cost effective, less obtrusive, and more 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.

A careful review of the prevalent threat environment and consideration of minimum applicable standards prior to finalization of plans will help to determine an airport's most appropriate security posture. Such a review may also help to reduce a later reliance on labor-intensive procedures and equipment. Inclusion of airport security expertise early in the planning process will result in a better-coordinated and more cost effective approach to security.

This Recommended Security Guidelines document is intended to help the user ensure that security considerations and requirements are a component of the planning and design of airport infrastructure, facilities and operational elements.

Section B - Applicability

These recommended guidelines are provided for consideration by aviation user-agencies (*airport operators*, *aircraft operators*, *airport tenants*), airport planners and consultants, designers, architects, and engineers engaged in renovation and new airport facility planning, design or construction projects. Some of the recommendations contained in these guidelines 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 current and future physical and procedural security consequences. In addition, the concepts found in this document may be considered when performing assessments of airport security and/or vulnerability.

Certain portions of this document outline procedural aspects of operational processes, extending beyond the proposed design and construction concepts. These are integrated here as a brief tutorial in operational subject matters that may be little known to the designer/architect. The drafters consider it very important to understand the

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

This document provides guidelines and recommendations only and is not intended to suggest mandatory measures for any airport. Although this document contains information of interest primarily to commercial airports regulated under Title 49 of the Code of Federal Regulations (CFR), Part 1542 (hereafter referred to as 49 CFR 1542), some suggestions may be useful for consideration by general aviation (GA) airport operators as well.

GA airports may also refer to a document developed by a different ASAC working group in 2004, titled *Security Guidelines for General Aviation Airports*. To obtain a copy of *Security Guidelines for General Aviation Airports*, contact the General Manager for General Aviation, Transportation Security Administration.

Section I-B - Applicability Checklist:

☐ **Airports**
- New
- Existing
- Expanding
- Commercial Passenger
- General Aviation
- Major Cargo
- Multi-Modal

☐ **Users of this Book**
- Airport Operators
- Aircraft Operators
- Airport Tenants
- Planners
- Designers
- Architects
- Engineers
- Consultants

☐ **Projects**
- Planning
- Design
- Construction
- Renovation
- Assessment

☐ **Facilities**
- Terminals
- Cargo/Freight
- Police/Fire
- Maintenance
- Catering
- Roadways/Parking
- Tenant and Other On-Airport Facilities

Section C - Purpose

The purpose of this document is to provide guidance for professionals responsible for, and affected by, the planning and design of airport facilities. Use of this document at the start of the airport planning and design process helps ensure that security needs are adequately considered.

This document contains "checklists" to ensure the 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 or change orders. Likewise, security features which have been coordinated early in the planning and design process with the TSA, Federal Aviation Administration (FAA) and other concerned regulatory bodies, as well as with airport tenants (aircraft operators, catering, concessions) and end-users (law enforcement, public safety and regulatory agencies, and airport operations and maintenance personnel) are more likely to be well-received and accepted, and thus more widely used and successful.

These guidelines identify key security concerns and concepts that should be factored into the planning and design of airport facilities. Essential considerations include:

1. Access to the *Air Operations Area (AOA)*, *Security Identification Display Area (SIDA)* and *Secured Area*, which are defined in 49 CFR 1540 and 1542;

2. Flow of people from *landside* to *airside* and from airside to landside;
3. Efficient *security screening* of persons and property into *sterile areas* as described in 49 CFR 1540, including consideration for queuing space during peak loads;
4. Separation of *security areas* and/or use of required and recommended signage (static and dynamic), as required;
5. Protection of *vulnerable areas* and assets;
6. Protection of aircraft, people, and property;
7. Blast mitigation measures;
8. Space for checked baggage Explosives Detection Systems (EDS) and devices;
9. Space for Explosives Trace Detection (ETD) equipment at screening points;
10. Space for Explosives Ordnance Disposal (EOD) operations such as robots and Threat Containment Units (TCU).

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. There may numerous solutions to any security challenge, and architects, planners, and designers are urged to examine and consider all potential avenues before selecting the solution that best addresses their airport's needs in a responsive and cost-effective manner.

Users of these guidelines are reminded that the application of physical security equipment and structures (barriers, access control, screening, and detection equipment) is fully effective only if supported by similarly effective human procedures. These include access and identification (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 code officials, building code officials, emergency response agencies, operations and maintenance personnel, and other end-users should occur for effective and efficient airport security.

This document is designed to be used primarily in digital/electronic form, although it is also easily used by hard-copy readers. In the electronic version, listings in the Table of Contents are dynamically linked to the internal section listed. Simply click on the title heading and you will be taken to that section of the document. To return to the Table of Contents, click the browser's "back" or "return" button.

Within the body of text throughout the document, you will find language with hyperlinks underlined in blue italics referring the reader to other related sections and topics. For example, where terminology is being defined and/or used the first time, or where reference to the complete definition is deemed useful, a hyperlink is provided to that term's location in *Appendix E - Glossary*.

Section I-C - Purpose Checklist:

☐ **Identify Key Concerns & Concepts in order to:**
- Restrict access to the AOA, SIDA & Secured areas
- Control the flow of people
- Provide efficient security screening
- Separate security areas
- Protect vulnerable areas & assets
- Protect aircraft, people & property
- Address blast mitigation measures
- Provide space for EDS & ETD devices
- Provide space for EOD operations

☐ **Identify Early Coordination needs with:**
- Airport Law Enforcement
- Emergency Response Agencies
- Fire Code Officials
- Building Code Officials
- Model Code Officials
- Operations and Maintenance Personnel
- Other End-Users

Section D - Background

The *Aviation Security Improvement Act of 1990*, Public Law 101-604 directed the FAA to work with the aviation industry to develop guidelines for airport design and construction to allow for maximum-security enhancement. This legislation was influenced by recommendations made by the President's Commission on Aviation Security and Terrorism and recognized that the designs of many airport structures did not accommodate the application of appropriate security measures at that time.

The *Aviation and Transportation Security Act of 2001 (ATSA)*, Public Law 107-71 established the TSA. The act authorizes increased federal responsibility for all aspects of aviation security, including a federal take-over of passenger and baggage screening. The responsibilities of TSA were defined further in 2002 with the passage of the *Homeland Security Act*, Public Law 107-296, which created the DHS. The primary missions of the department include preventing terrorist attacks within the United States, reducing the vulnerability of the United States 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 bill: information analysis and infrastructure protection; chemical, biological, radiological, nuclear (CBRN), and related 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.

Following creation of the DHS and the TSA, there has been a focus on protecting the national transportation system infrastructure as a whole. The federal government has required various agencies to jointly develop national strategies and plans to ensure an intergraded approach to transportation security. Additional information on these plans and other specific pre-planning considerations should be coordinated with the TSA Federal Security Director (FSD) responsible for the airport.

Newly available technological tools for vulnerability/risk assessment, flow modeling, and bomb blast protection can reduce guesswork and minimize certain expenditures in new structures. (Refer to *Appendix A – Airport Vulnerability Assessment Process*, *Appendix B – Airport Security Space Planning*, and *Appendix C – Airport Blast Protection* for further information.)

Section E - Coordination

For new construction or extensive renovation, airport facility planners and designers should encourage the early formation and involvement of an *Airport Security Committee*. The committee should include the affected aircraft operators and tenants, fire code officials, building code officials, local FAA and TSA, local emergency response agencies, aviation security and other regulatory officials. Its role is to assist planners and designers to factor the appropriate security and safety perspective into designs for current security concerns and to accommodate anticipated long-term expansion and regulatory changes where possible. Early security-oriented reviews of design plans can alert project managers to potential integrated security approaches that may be effective as well as 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 could include recommended countermeasures.

Careful attention must be given to coordination with the regulatory requirements found in *49 Code of Federal Regulations (CFR) 1540, 1542, 1544, 1546 and 1548* (hereafter referred to as *49 CFR 1540, 49 CFR 1542, 49 CFR 1544, 49 CFR 1546 and 49 CFR 1548*), and the sometimes-overlapping areas of control and managerial jurisdiction spelled out in the respective airport's *Airport Security Program (ASP)*.

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 – U..S. Customs and Border Protection (CBP), U.S. Fish and Wildlife Service (FWS), and Public Health Service (PHS) – operating at airports are addressed in the *CBP Airport Technical Design Standards* For Passenger Processing Facilities and separate FWS and PHS standards respectively. These Standards contain the physical characteristics of the FIS area and set forth requirements for the design of new or remodeled airport terminal building facilities to accommodate CBP processing of international passengers and their luggage arriving in the U.S.

The *CBP Airport Technical Design Standards* discuss passenger and baggage flow and terminal building space utilization including space guidelines for processing arriving international passengers and baggage as well as offices, processing booths, counters, conveyors, security requirements, x-ray systems, access control and other equipment necessary to support the monitoring, control, and operation of the FIS facility. As of late 2005, the *CBP Airport Technical Design Standards* were being composed by CBP to incorporate the legacy Agriculture, Customs, and Immigration facility standards into one set of comprehensive CBP standards that will replace legacy agency standards.

Airports, planning-architectural-engineering firms, and other interested parties should contact CBP Headquarters for information and guidance relating to the application and interpretation of the Legacy Agency (Agriculture, Customs, and Immigration) standards on affected airport projects early in the planning and design process.

The reader should refer to the most current FIS guidelines when accommodating those agencies' requirements in an airport design. For related information contained within this document, refer to *Federal Inspection Services Areas* on page 80.

Section I-E - Coordination Checklist:

- ☐ **Initial coordination with the TSA FSD**
- ☐ **Get the early involvement of Airport Security Committee & others**
- ☐ **Assure 49 CFR and ASP requirements are met**
- ☐ **Consider the needs of law enforcement, emergency response, security and safety support personnel**
- ☐ **Reference *CBP Airport Technical Design Standards* at Airports where FIS areas are involved**

Section F - 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 and the FAA's airport representatives to ensure designs facilitate the implementation of local airport (including affected foreign air carriers) and aircraft operator *contingency measure* requirements.

1. Homeland Security Advisory System (HSAS) Threat Conditions

The U.S. DHS HSAS is composed of five threat conditions, each representing an increasing risk of terrorist attack:

a. Low Condition **GREEN** – low risk of terrorist attack

b. Guarded Condition **BLUE** – general risk of terrorist attack

c. Elevated Condition **YELLOW** – significant risk of terrorist attack

d. High Condition **ORANGE** – high risk of terrorist attack

e. Severe Condition **RED** – severe risk of terrorist attack

2. TSA Responsibilities

Airport operators, in consultation with their FSD, must develop and incorporate into their TSA-approved ASP, Aviation Security (AVSEC) Contingency Plans that are tailored to the airport. AVSEC systems, methods and procedures should address specific HSAS levels. In developing the plan, the airport operator and FSD must 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.

When the Secretary of the Department of Homeland Security declares the nation at an enhanced threat condition, the airport operator and others must immediately implement the corresponding security measures contained in the AVSEC Contingency Plan and all appropriate security directives.

In addition, the airport operator is responsible to ensure that an FAA-approved Airport Emergency Plan (AEP), is coordinated with the TSA FSD and included in the overall Airport Operations Manual for FAA certification of the airport. The AEP will identify the local emergency response agencies (hospitals, emergency medical services, mutual-aid first responders, military and federal support agencies, etc.) and types of services which will need to be accommodated and may require additional facilities during emergency conditions.

3. Planning and Design Considerations

Consideration should be given to the systems, methods and procedures that may be required by the airport, aircraft operators and tenants to implement AVSEC measures approved within their various security programs. AVSEC measures are intended to be temporary operational security enhancements; however design and construction of facilities and infrastructure may ensure more efficient implementation or operational control.

Section I-F - Security Concerns & Contingency Measures Checklist:

- ☐ **Discuss contingency needs with airport, TSA, FAA and aircraft operator officials**
- ☐ **Consider potential impact of contingency measures and emergency plans**
- ☐ **Consider potential impact on various areas (landside, airside, terminal, etc.)**
- ☐ **Consider the latest changes in security concerns**

PART II

INITIAL PLANNING AND DESIGN CONSIDERATIONS

Section A - 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 specific FAA Advisory Circulars (A/C) for various elements that need to be considered from initial planning through completion of a specific project. Since the creation of the TSA, the authority to ensure the inclusion of security systems, methods and procedures within this construction and operational process is the responsibility of TSA.

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

Planning for security should be an integral part of any project undertaken at an airport. The most efficient and cost-effective method of instituting security measures into any facility or operation is through advance planning and continuous monitoring throughout the project. Selecting, constructing, or modifying a facility without considering the security implications of the general public and airport personnel can result in costly modifications and delays.

Physical security approaches should be based on applicable federal, state, and local regulations and policies to ensure the protection of the general public, airport personnel, and assets (including information systems and data). At a minimum, a physical security approach should include:

1. A vulnerability assessment (refer to *Appendix A*) to evaluate the security of an existing airport or a comprehensive security prospectus evaluating a new facility or site;
2. Periodic inspections to ascertain whether a security program and its implementation meet pertinent federal, state, and local standards or regulations;
3. A comprehensive and continuing security and threat awareness and education effort to gain the interest, support and participation of employees, contractors, consultants, and visitors;
4. Implementation of procedures for taking immediate, positive and orderly action to safeguard life and assets during an emergency.

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

To ensure a systematic approach to acquiring and analyzing the information necessary to support decision-makers in the protection of assets and the allocation of security resources, all security specialists should refer to the applicable federal, state, and local requirements and standards referenced in this guide.

Finally, airport security should reflect the risk status and financial resources of an airport. More than 90 percent of the air carrier airports in the U.S. are small or medium hub airports which may have limited funding and have to plan their security projects with an eye toward simplicity and manageable cost.

Section II-A - General Checklist:

- ☐ **Advance Planning**
- ☐ **Continuous Monitoring**
- ☐ **Physical Security Program**
  - Vulnerability assessment
  - Periodic inspections
  - Continuing security awareness/education
  - Emergency procedures
- ☐ **Consult with Experts in Aviation**
- ☐ **Coordinate with Security/Regulatory Personnel**
- ☐ **Refer to Regulatory Requirements & Standards**
- ☐ **Coordinate with the TSA FSD**

Section B - Facility Protection

The airport has a responsibility to provide a safe operating environment and infrastructure. The extent of facility protection should be examined by the local *Airport Security Committee*, considering the results of a comprehensive security prospectus of the new facility or *vulnerability assessment* of the existing facility. High priority should be placed on protection of the aircraft from the unlawful introduction of weapons, explosives, or other threatening articles. Refer to *Appendix A – Airport Vulnerability Assessment Process* for further information.

Perimeter protection (fences, gates, patrol) is the first line of defense in providing physical security for personnel, property, and information at a facility.

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

Section II-B - Facility Protection Checklist:

- ☐ **Airport Security Committee Review**
- ☐ **Perimeter Protection - First Line of Defense**
- ☐ **Interior Controls - Second Line of Defense**
- ☐ **Cost Analysis**

Section C - Planning Facility Protection

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

1. General Security Areas and Boundaries

Several elements or components of an airport operation should be considered when planning for the protection of an airport facility. *Figure II-C-1* below is a general depiction of the different areas at a typical commercial airport, such as a terminal, aircraft apron, runways or taxiways, and many other components which are typically more comprehensively shown on an FAA-approved Airport Layout Plan (ALP). The ALP might be one of the first documents suggested for review that will show the airport property and the facilities at a particular airport.

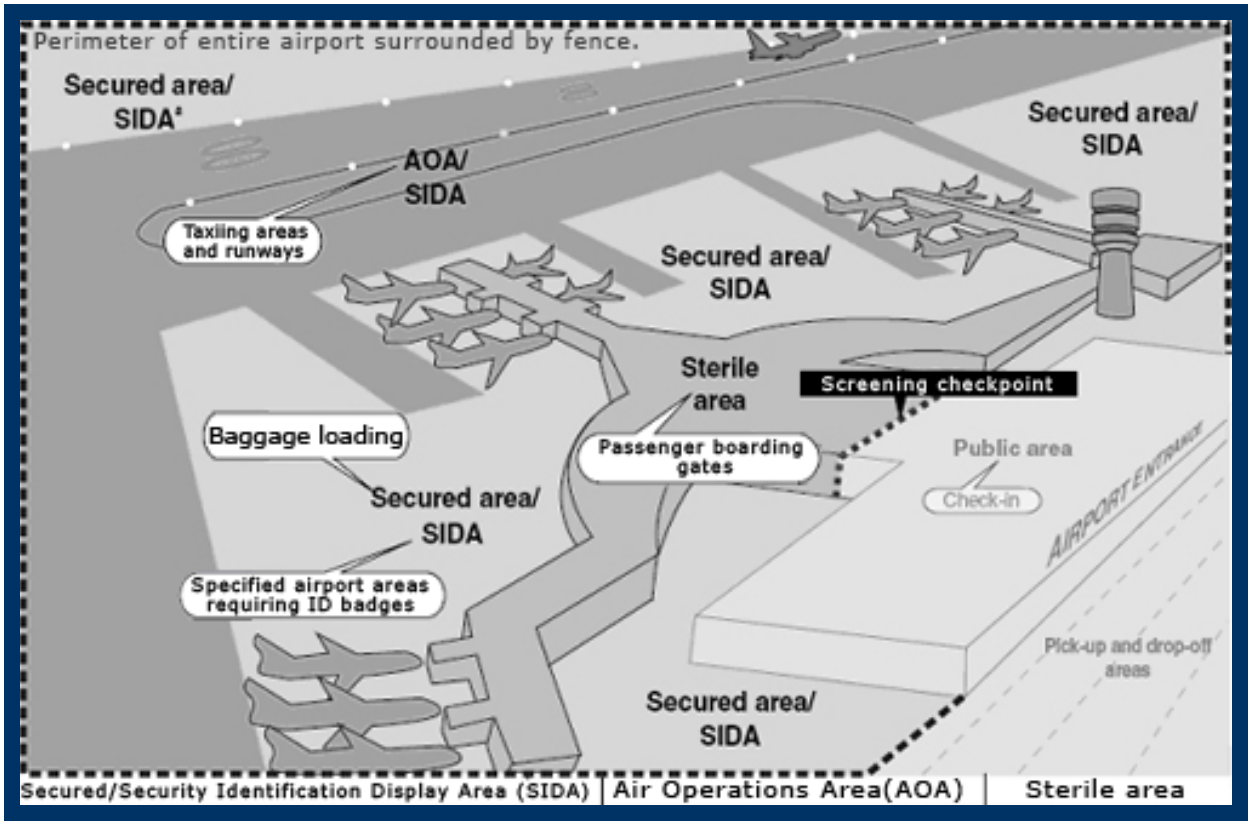


Figure II-C-1 - Security Areas General Depiction

a. Establishment of Security Areas and Boundaries

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, but in many instances, boundaries may not be hard physical barriers, such as fences or walls; they might instead be painted lines, lines marked and monitored by electronic signals, grass or pavement edges, natural boundaries such as water or tree lines, or simply geographic coordinates.

b. Security Areas Basic Requirements*(refer* to *501HSecurity Area Descriptions* on page 15 for additional information)

Table II-C-1 below provides general comparative descriptions and regulatory requirements (including training, criminal history record checks (CHRC), and ID display) for the three basic airport security areas: Secured Area, SIDA, and AOA. Please discuss security areas at a specific airport with the local airport security coordinator and local FSD for further clarification. Note: Some designers use the term 'restricted area', but that is a broad generic term and does not carry a specific definition in U.S. airport regulations.

(refer to *Security Area Descriptions* on page 15 for additional information)

Table II-C-1 - Security Areas Basic Requirements and Descriptions

	Secured Area	SIDA	AOA
Regulatory Requirements	*Requires:* 1) Access controls meeting 49 CFR 1542.207 performance standards 2) Security Training 3) Full CHRC 4) ID Display/Challenge	*Requires:* 1) *No access control required* 2) Security Training 3) Full CHRC 4) ID Display/ Challenge	*Requires:* 1) Basic access controls meeting 49 CFR 1542 2) Provide Security information
Securtiy Level	Relatively high level of security including access controls, training, CHRC and ID display/challenge.	SIDA relates to ID display and CHRC only. Access controls are determined by requirements of AOA or secured area location in relation in to the SIDA.	Broadest application of security; requirements are not specifically set forth in 1542.
Relational Description	A Secured area is always a SIDA, because all 3 required SIDA elements are present- Training, CHRC, and ID display/challenge. However, the Secured Area goes beyond SIDA by also requir-ing access controls.	SIDA lacks access controls, so a SIDA, by itself, cannot, be a secured area.	The AOA requires only basic access controls, but sets no specific standards.

2. Vulnerability Assessment

A *vulnerability assessment* can be an excellent tool to assist in determining the extent to which a facility may require security enhancements, and serves to bring security considerations into the mix early in the design process rather than as a more expensive retrofit. Many tools and methodologies are available; all are subjective to varying degrees, largely because in every case, one must first have a firm grasp of both short and long term threat in order to ask the necessary first three questions: "What is the threat?", "What is an airport's level of vulnerability relative to that threat?", and "To what extent will the threat/vulnerability change?" The planning and design team's response to these questions will be a recommendation of a combination of security measures, both physical and procedural, seeking balance between strong security and ease of movement for both

passengers and employees. Refer to *Vulnerable Areas* on page 17 and *Appendix A – Airport Vulnerability Assessment Process* for further information.

3. Protection Criteria

The Airport Security Committee may offer recommendations on the level of normal protective service, and may consider the following:

a. Known threat(s) specific to the airport and/or to the airlines serving it;
b. History of criminal or disruptive incidents in the area surrounding the facility, but not primarily directed toward airport operations;
c. National threats and the general integrity of U.S. Transportation
d. Facility location, size, and configuration;
e. Extent of exterior lighting;
f. Presence of physical barriers;
g. Presence of access control and alarm monitoring systems (ACAMS), closed-circuit television (CCTV) systems, and other electronic monitoring systems;
h. Presence and capabilities of on-site staff and/or security patrols; and
i. Other locally determined pertinent factors, such as general aviation (GA), commercial operations, etc.

4. Physical Protection

Airports and aircraft operators provide normal and special protection through a combination of: mobile patrol 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 crime prevention assessment. Refer to *Appendix A* for further information.

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 occupant and federal agencies upon request, and conduct crime prevention assessments in cooperation with appropriate law enforcement agencies.

6. Recordkeeping

In addition to physical protection and other protection and prevention criteria, airports may also have a need to keep records of incidents, personnel access, or other activities. Some of the records (such as personnel access) may be maintained automatically and/or electronically. In such cases, recordkeeping needs may affect designs and equipment locations as well as require considerations for secure data storage and should be coordinated early in the design process.

7. Delegations of Responsibility

Some security responsibilities under 49 CFR 1542 may be transferred to a tenant or aircraft operator. Normally, the airport will retain responsibility for law enforcement, monitoring of alarms, requests for criminal investigations, and fire and facility safety and health inspections. This type of agreement between airport and aircraft operator is known as an *Exclusive Area Agreement*, or in the case of other airport tenants, an *Airport Tenant Security Program (ATSP)*. There may also be *Letters of Understanding* among nearby jurisdictions to provide assistance to each other during emergencies, but typically these are simply promises to give aid, not delegations of authority.

8. Design Factors

It is important to consider security systems and procedures from the design phase on, 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 a paramount concern in design and construction of an airport facility. For this reason a brief discussion of seismic requirements appears in *Seismic Requirements* on page 20.

Section II-C - 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
  - Wiring Requirements
  - Heavy-load Equipment
  - Effects on Passenger Flow
  - Construction Equipment Needs
  - Large-size Material Delivery
  - Seismic Requirements

PART III

RECOMMENDED GUIDELINES

Section A - 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 the 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 assure that the airport's needs are met, particularly since aviation security requirements and surrounding environments may frequently change.

1. General Airport Layout

The general layout of an airport consists of three (3) areas generally referred to in 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, terminal) has its own special requirements. Airside/landside requirements and operational parameters should be carefully considered when planning and designing a new airport or facility. The requirements, barrier 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.

a. *Airside*

The airside of an airport is 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 which service and maintain aircraft. For operational, geographic, safety, or security reasons, other facilities such as tenant and cargo facilities may be located within the airside as well.

As the airside generally includes security areas to which certain requirements apply under 49 CFR 1542; e.g., the Aircraft Operations Area (AOA), Security Identification Display Area (SIDA) and Secured Areas, the airside, by nature, must be nonpublic. Further information on these security requirements is contained in *Security Areas* on page 15.

The choice as to where this airside perimeter fencing or barrier may be located is often subject to the surrounding environment and access roads and may be one of the most critical decisions in designing or renovating an airport. In addition to the factors discussed in *Facilities, Areas and Geographical Placement* on page 41, the following factors should be considered when determining airside boundaries and orientation:

1) Dangerous or hazardous areas that could affect the safety or security of a parked or moving aircraft;

2) Concealed/overgrown areas that could hide persons or objects that might endanger aircraft or critical airport systems;

3) 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;

4) 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.)

5) 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 airside must be able to maintain required operational clear areas, have adequate emergency response routes and response times, and have in place required safety measures.

b. *Landside*

Excluding terminals, which are treated separately below, the landside of an airport is that area of an airport and buildings to which both traveling passengers and the non-traveling public have unrestricted access. Typically, the landside facilities include patron and other public parking areas, public access roadways, rental car facilities, taxi and ground transportation staging areas, and any on-airport hotel facilities.

Since the landside includes all non-airside areas (other than the terminal(s)), its location is determined by the airside and perimeter boundary. Within landside, factors affecting the location of facilities are discussed in *Facilities, Areas and Geographical Placement* on page 41

Since the landside is not directly affected by the operation of aircraft, it generally has less stringent security requirements than the airside. However, some clear area and communication requirements may still affect landside design and layout, 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* on page 15.

The landside in general 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.

c. Terminal

An airport terminal is a building or buildings designed to accommodate the enplaning and deplaning activities of aircraft operator passengers. Larger airports or those with general aviation areas often have more than one terminal. For purposes of this document, the term "terminal" typically refers to that main building or group of buildings where the boarding of public, scheduled commercial aircraft occurs or from which persons who have passed through a security screening process will proceed to boarding facilities located elsewhere on the airside.

When considering passenger and baggage screening security provisions, it is important for planners and designers to distinguish the commercial terminal from the general aviation terminal where charter and private passenger activity typically occur. However, 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 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 typically the area of the airport with the most security, safety, and operational requirements. Many of these requirements are closely linked to the location of *security areas* within, and in close proximity to, the terminal. Since the terminal usually straddles the boundary between airside and landside, certain portions must meet the requirements of both of these areas.

When designing a new facility, the terminal should be 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 (DDR) to

unauthorized penetration. Providing additional "standoff" distance from a potential Large Vehicle Improvised Explosive Device (LVIED) 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.

Section III-A-1 - Airport Layout and Boundaries Checklist:

☐ **Analysis of General Security Requirements**

☐ **Security & Safety Considerations**
- Separate dangerous or hazardous areas
- Minimize concealed/overgrown areas
- Effects on/by adjacent facilities
- Natural features that might allow access
- Prevent communications interference due to natural features, buildings & equipment
- Public safety & security concerns
- Criminal Activity

Airside
- Nonpublic
- Maintain airside/landside boundaries
- Maintain security clear areas and zones
- Adequate emergency response routes
- Required safety measures & 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 & safety
- Public security & safety

2. *Security Areas* (Refer also to *Figure II-C-1* on page 9)

The Airport Security Program (ASP) required under 49 CFR 1542.101 contains specific descriptions of the following areas in which security measures are specified in 49 CFR 1540.

a. Air Operations Area (AOA)

An AOA is a portion of an airport, specified in the ASP, 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 and 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.

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, but rather, leaves the solution to the local authorities, subject to TSA approval.

In most cases, it is advantageous to align the AOA boundary with other boundaries or with physical barriers. Typically, 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 are being used to delineate boundaries. The AOA is required to have a distinct, securable boundary line. Refer to *Boundaries* on page 22 for more information.

When allocating AOA space, and since the AOA requires less specific security measures than SIDAs or secured areas, consider whether to locate construction staging areas, in-flight kitchens, commissaries, and other facilities outside those critical areas within the AOA. This will facilitate implementation and may reduce the cost of access control and identification system measures for such areas. Locating most non-terminal areas outside of the SIDA may also reduce the amount of man-hours needed for identification media issuance and revalidation, background checks, and security training. Further discussion on *Facilities, Areas and Geographical Placement* is included on page 41.

b. Security Identification Display Area (SIDA)

A SIDA is 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. Generally, the SIDA is an area requiring display of an authorized identification media.

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; a secured area is by definition always a SIDA, in that all SIDA requirements within 49 CFR 1542.205 must be met within a secured area.

In general, 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.

c. 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, deplane passengers and sort and load baggage, and 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 (LEO) response, display of ID, etc., particularly where the various secured areas may not enjoy common boundaries or access points. A secured area is by definition always a SIDA, in that all SIDA requirements within 49 CFR 1542.205 must be met within a secured area.

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 access by response personnel, utilize common areas of closed circuit television (CCTV) surveillance coverage, and minimize requirements for redundant boundaries and electronic access controls. Where there are several unconnected secured areas - baggage makeup areas, movement areas, safety areas, etc. - each may require separate but integrated electronic controls.

d. Sterile Area

A Sterile Area is a portion of an airport, specified in the airport security program 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, the aircraft operator, or designated foreign air carrier must use adequate facilities and procedures to screen persons and property prior to entry into the Sterile Area to prevent or deter the carriage aboard aircraft 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. These 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. Sterile areas may include various revenue-generating facilities, particularly concessions, 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.

e. Exclusive Area

An Exclusive 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 49 CFR 1546 has assumed responsibility under 49 CFR 1542.111.

Within the Exclusive Area, the responsible signatory aircraft operator or designated 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 approved by TSA. Such conditions include a delineation of very specific areas for which the aircraft operator assumes

security responsibilities. Like SIDAs and Sterile Areas, Exclusive 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.

f. Airport Tenant Security Program (ATSP) Area

An ATSP Area is an area specified in an agreement between the airport operator and an airport tenant that specifies the measures by which the tenant will perform specified security functions, authorized by the TSA, under 49 CFR 1542.113.

Subject to a tenant-area-specific security program approved by TSA, the airport tenant has responsibility for specific security systems, measures or procedures.

Where tenants other than air carriers elect to undertake under their own security programs 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.

Section III-A-2- Security Areas Checklist:

- ☐ **AOA**
  - Align AOA boundary with fences or natural boundaries
- ☐ **SIDA**
  - Part of AOA
  - Smallest manageable contiguous size(s)
- ☐ **Secured Area**
  - Consider general aviation, cargo, maintenance, and other facilities in a manner consistent with latest TSA regulation and policy guidance.
- ☐ **Sterile Area**
  - Minimize size to help surveillance and control
- ☐ **Exclusive Area**
  - Minimize areas to be monitored/controlled
- ☐ **ATSP Areas**
  - Minimize areas to be monitored/controlled

3. Assessment of Vulnerable Areas

a. Basic concepts of security risk management dictate that the security system provide the appropriate level of security to all of the assets to be protected, in light of the perceived threat to those assets. Therefore, at the facility planning stage it is prudent to consider all of the assets (or targets of a terrorist or criminal attack), considering their relative "value" (or consequence of loss) and economical impact. There are many possible high value assets at an airport to consider, such as: aircraft (with or without passengers aboard); air traffic support facilities (tower, radar, weather, communications); terminal building(s), groups of members of the public or employees; fuel storage; critical infrastructure (power, water, communications) and railway, roadway or vehicle access way and surrounding waterways/intermodal transportation facilities.

b. 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 (such as the AOA, Secured Areas, SIDA, ATSP Areas and Exclusive Areas). Since barriers and controls are required to differentiate these areas and to limit access to them, this may lead to the assumption that anyone or anything found in the area is authorized. This suggests a common vulnerability; once inside the controlled area, an intruder may move about without encountering additional controls. For example, if an intruder breaches the fence line (considered to be easily and quickly achieved), he may find no further physical barriers to control access to aircraft, the baggage makeup area (BMA), 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.

c. Other means of achieving unauthorized access exist, such as through reverse use or other misuse of emergency exits (for example, from public side to the secured area) or unauthorized use of a controlled access portal opened by an authorized user, a practice often called "piggybacking." New construction designs 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 should be supported by comprehensive surveillance (such as CCTV) on both sides of the door for alarm assessment. Ideally the airside surveillance would include an intruder tracking capability to allow for directing the response force. Attentive planning and incorporation of appropriate surveillance or control devices can significantly improve the identification and control of piggybacking, as well as the deployment and efficient use of manpower resources to respond to anomalies. Contact the airport security coordinator and local FSD for current sensor evaluation (pilot program) reports that may be applicable at a particular airport.

d. Another area of concern is unauthorized entry or breach in 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). From the planning and design standpoint, the most significant considerations for implementing a physical breach control system are: 1) source and location of breach identification alarm generator; 2) location of physical barriers which respond to the breach alarm; and 3) sufficient separation distance between 1 & 2 to allow safe and sure closure prior to intruder's further penetration which could result in terminal evacuation. Other concerns such as fire and safety codes must also be considered.

e. All public access facilities, within which large congregations of people are customary, suffer from a fundamental vulnerability to terrorist bombing or armed attack. 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. [Refer to charts in *Appendix C*]. 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 to redirect or otherwise mitigate blast effects.

f. The threat of an armed attack on the terminal as well as the threat of 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 congregations are expected, there are limited means by which a security system can prevent an attack. To assure that LVIEDs, IEDs, or terrorists with weapons do not enter the terminal requires moving the point of screening "to the front door." Here again, architects and designers may seek innovative designs that can accommodate all of the passenger convenience issues, as well as accommodating screening of all people and items before entering the terminal (creating a "sterile terminal"), to significantly reduce this vulnerability. Many other issues that may not be readily apparent require that a "front door" option be carefully considered in close coordination with aircraft operators, the airport authority, and the local FSD.

g. A potential vulnerability also exists at any facility using an access media/identification system that grants access privileges to employees and others. These "insiders" have legitimate needs to access the portions of the airport controlled for security purposes and are granted access to those areas, and in some cases to the workings of the security system itself. However, threats from insiders, acting alone or in collusion with outsiders, pose a criminal and terrorist threat to airports. The need to inspect individuals, their identification media, and their possessions as they cross the security boundary using their access privileges, may increase in the future. The need to identify and control individuals under escort within the controlled portions of the airport may also increase in the future, 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 access points that employees use to gain access to their work site in the secure area. 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. Although challenging in the absence of specific security requirements, designers and planners should consider throughput in the event security requirements are mandated for employee access portals.

h. 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

general aviation facilities, commercial and industrial buildings, etc., which, while not necessarily recognized as a target of terrorist activity, might still be in the path of such an attack, or at the very least might be subject of common crime such as theft or vandalism, and thus might require varying levels of security protection. These may or may not fall under the jurisdiction or responsibility of the airport, 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 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.

i. Utility Infrastructure

1) Utility sources, equipment and supply potential should be protected and/or monitored to the extent warranted by a threat and vulnerability assessment. 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.

2) In this context, 'utilities' encompasses 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 Cooling (HVAC).

3) 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 switching capability. Individual battery back-up or UPS units to support access control systems during power outages are also highly desirable. Furthermore, the security design must provide distributed essential power for priority provisions (i.e., lighting, communications, etc.). Consideration should also be given to providing essential power to support defined secondary (limited use) requirements that may be needed during outages.

4) HVAC systems have important functions during extreme weather conditions because they control and maintain ambient temperatures for thousands of passengers and employees. HVAC equipment provides fresh air or heat circulation, and an attractive target or vector for attack. The security design should consider providing a capability to monitor publicly accessible air intakes (e.g., use of video cameras), the capability to isolate sections of the building, and to extract and vent sections of the building by using a positive air pressure. *See Appendix G, Airport Chem-Bio Protection and Response.* For more on design to prevent or mitigate chem-bio events.

5) Tunnels and drainage provisions provide apertures into the building that may be exploited by an adversary. Airport design should consider the security of the routes by which utilities enter and exit the terminal building.

6) Fuel supplies may support vehicle and/or aircraft operations that require protecting the pipelines, fuel farms, or other facilities that are operationally sensitive and vulnerable to attack.

7) Water sources may merit protection, keeping in mind the function of the water. Whether water's 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. An alternative source of water may be appropriate, particularly for fire-fighting and other emergency purposes.

8) 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 should be designated as

"critical assets" and secured by ACAMS and CCTV systems in the same manner as other critical airport facilities. When network cabling traverses public areas, metal conduit should be used to protect the cabling.

9) 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 should also support airport operations and other departments. Dependence on carrier cellular services should be minimized as these networks can be 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.

10) Seismic Requirements

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

This section provides information referencing 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 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 refer to further resources for information or expert opinion about the appropriateness and effectiveness of any specific seismic requirement as it affects their airport design. It is also important to note that the burden of conformance may rest solely on the Architect, Engineer and Contractor and to remember that the guidelines and regulations supporting the implementation of individual acts often contain the most important detail.

In recent years enforcement of the earthquake protection requirements in the Model Codes for nonstructural building components has also become commonplace. Model Codes provide for nonstructural, infrastructure elements of the building design, such as electrical enclosures, control consoles, conduits, cable trays, etc. Architects, Engineers and Contractors are relied upon to know, understand, design and install earthquake protection in accordance with the requirements of these Codes.

It is important to note that all of the Seismic Laws and the 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. Although the following list is not intended to be comprehensive and complete, as an aid to the designer, the TSA recommends that the following sources of information be checked to determine the requirements to be applied.

a) Public Laws 95-124 and 101-614 "The Earthquake Hazards Reduction Act of 1977 as Amended"
b) Executive Order 12699 of January 5, 1990 "Seismic Safety of Federal and Federally Assisted or Regulated New Building Construction"
c) Executive Order 12941 of December 1, 1994 "Seismic Safety of Existing Federally Owned or Leased Buildings"
d) ICBO (International Conference of Building Officials) "Uniform Building Code (UBC)," 1994, and amendments to include the 1994 NFPA-13 Standard for Building Fire Sprinkler Systems
e) BOCA (Building Officials Code Authority) "National Building Code"
f) SBCCI (Southern Building Code Congress International) "Standard Building Code"

g) Section 13080 of the Corps of Engineers Guide Specifications with Fire sprinkler Sections 15330, 15331, and 15332 revised in March 1995 to unequivocally require seismic bracing on the small diameter piping.

h) Various State Building Codes, e.g., California, Washington, Alaska, Missouri, New York, etc., which may require mitigation elements in addition to the national standards.

Section III-A-3 - 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 Way
  - 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
  - Delays
  - Piggybacking
  - Surveillance/CCTV
- ☐ **Plan for breach control measures and procedures**
  - Physical Barriers
  - Separation Distance
- ☐ **Reduce bombing/armed attack vulnerability**
  - Blast Mitigation
  - Separation Distance
  - Minimization of 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**

4. Chemical and Biological Agents

When considering overall layout, it is prudent to take some precautions to prevent attacks by non-conventional means, such as the use of chemical and biological agents, to attack civil aviation. 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 *Terminal* on page 58) or persons in areas controlled for security purposes.

Some measures that should be considered to help mitigate a potential chemical/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/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 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 ground level, they should be protected if possible with screens or grates, and turned 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/biological agents.

Additionally, at the direction of the Department of Homeland Security (DHS) Science and Technology Directorate through the PROACT (Protective and Responsive Options for Airport Counter-Terrorism) program, the Sandia National Laboratories issued "Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism," co-authored with the Lawrence Berkeley National laboratories. These guidelines are available for review from the TSA Federal Security Director at your airport or directly from Sandia National Laboratories upon request. An extract of the Sandia National Laboratories document is available in *Appendix G* of this document.

Section III-A-4 - Chemical & Biological Agent Checklist:

☐ **Sources of guidance may include TSA, Federal Emergency Management Agency (FEMA), Federal Bureau of Investigation (FBI), Department of Energy (DOE), Center for Disease Control (CDC) and Office for Domestic Preparedness Support.**

☐ **The *Bibliography* lists several relevant chem.-bio documents.**

☐ **Report Card for *airport Chem-Bio Protection and Response***

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, alarms), and natural barriers in the planning and design process of an airport. Access points for personnel and vehicles through the boundary lines, such as gates, doors, guard stations, and electronically controlled or monitored portals must also be considered. In addition, there are other security measures which should be part of the design that enhance these boundaries and access points such as clear zones on both sides of fences, security lighting, locks, monitoring systems such as CCTV, 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 a boundary line must 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 must 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 and possible financial liability to the airport.

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 which can enhance them are described below:

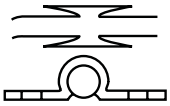
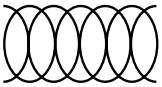
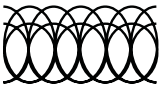
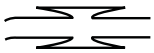
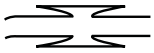
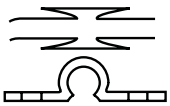
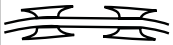
a. Physical Barriers

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.

1) Fencing

Fencing is available in several designs that are difficult to climb or cut as well as those which are provided with motion, tension or other electronic sensing means. For fences with sensors, either mounted on the fencing or covering areas behind fencing, there are other elements to the security system for monitoring of the sensors and response to intrusion alarms. *Table III-A-1* below shows some of the available types of fence fabrics.

Table III-A-1 - Fence Types and Fabric

	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″ - 16.67′ 9″ - 25′ 18″ - 50′	2800 lbs.
	RAZOR RIBBON MAZE - 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″ - 15′ 16″ - 20′	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″ - 15′ 16″ - 20′	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″ - 66′	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	24″ - 66′	2250 lbs.
	RAZOR RIBBON - Single Coil	Min. Security Fence Topping. Commercial Use	18″ 24″	9 lbs. 12 lbs.	AISI 430 Stainless Steel	6″ - 16.67′ 9″ - 25′ 18″ - 50′	1260 lbs.
	BAYONET BARB - Concertina	Ground Barrier	27 1/2″ 37 1/2″	23 lbs. 34 lbs.	ASTM A 526 Zinc Galvanized .098 dia. high Tensile Wire	20″ - 50′	1300 lbs.

Chain link fencing is a 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 7 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. Fences configured in this manner are shown in *Figure III-A-1* below.

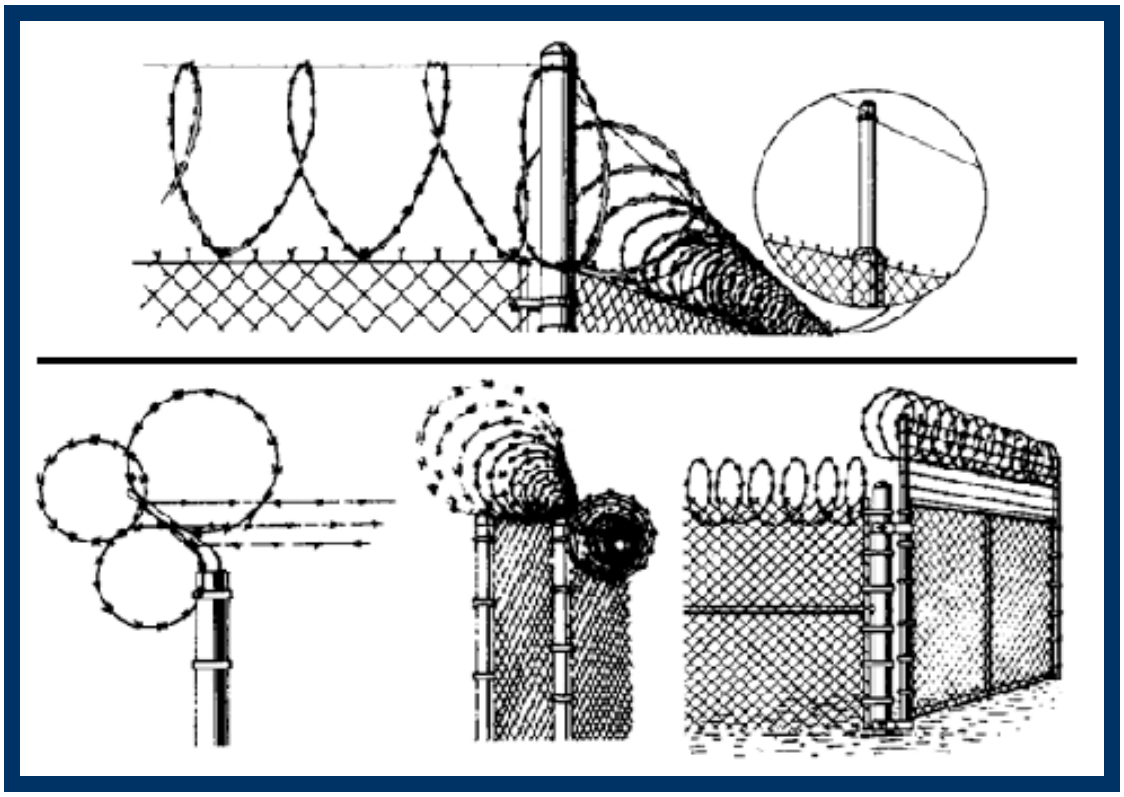


Figure III-A-1 - Chain Link Fence Barbed Wire Configurations

Chain link fencing is normally the most suitable and economic 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. On boundaries coinciding with property lines, locate the fence line should be located inside the airport property line to prevent encroachment on adjacent property by the barbed wire angled topping or its outriggers.

Another common type of fencing is constructed of vertical bars which have curved spiked tops as shown in *Figure III-A-2* below. Depending on the diameter and materials used for the bars, this design can provide additional protection against forced entry.

Figure III-A-2 - Vertical Bar Fence

There are several means of constructing fences to provide a higher level of protection against forced entry. Chain link fences, for example, can be reinforced with posts and rails, as shown in *Figure III-A-3* below, with rails being either solid material or stranded-steel cable encased in hollow pipe. The posts and rails can also be designed to blend into the fence. This type of reinforced fencing has been has successfully tested to the U.S. Department of State's K8 Anti-Ram rating, stopping a 15,000 pound truck traveling at 40 mph within 3 feet of the fence line.

Figure III-A-3 - Fence Post and Rail Reinforcement

When utilizing fencing as a security boundary, care must be taken to ensure that the provision of fencing does not conflict with the operational requirements of the airport. Access points must 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 must be planned for routine operations, maintenance operations, and emergency operations. For further information on fencing access points see *Gates* on page 29 or *Guard Stations* on page 31.

To assist in surveillance and security patrol inspection, keep fences as straight and uncomplicated as possible. This will minimize installation and maintenance costs.

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. A taut fence fabric is often required under such circumstances.

Effectiveness of fencing 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. Mowing strips may also reduce security and maintenance man-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 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.

In summary, fences are the most basic first line of deterrence and defense. There is excellent guidance available from the Chain Link Manufacturers Institute, including detailed technical and procurement guidelines and specifications such as the Security Fencing Recommendations..

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 be dependent upon the nature of the business being conducted inside, and the level of continuous access required by personnel.

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.

a) 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.

b) 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 exterior walls are less climbable and thus more secure 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.

b. Electronic Boundaries

In the case of boundaries which are monitored by electronic sensors, motion detectors, infrared or microwave sensors, etc., it is clear that these are intended to serve essentially the same security functions as other detectors, but are simply employing other technologies, usually with somewhat higher maintenance costs. Typically they will 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 involving existing FAA ground radar surveillance can be incorporated for use in a security mode. See also Radio Technical Commission for Aeronautics (RTCA) Document DO-221, "Guidance and Recommended Requirements for Airport Surface Movement Sensors."

1) New Electronic Boundary Technologies

This document is focused on planning and design during the initial planning for current projects, even though new facilities such as terminals may sometimes be 4 or 5 years from the drawing board to processing the first aircraft and its passengers. When planning that terminal, and all other related facilities requiring a security perspective, one must also take account of 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 easily 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 to monitor and respond to a wide range of alarms, including 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, nevertheless as new technology becomes tested and available, it may not only be useful but also very cost-effective to consider such expansion early-on when designing infrastructure such as cabling to perimeter locations, power sources, lighting, communications, and more, so as to avoid the need for such costly things as re-trenching, replacing limited panels, relocating camera positions, etc.

One such technology being tested in a major Category X environment is the adaptation of the existing FAA ASDE ground surveillance radar signal to also monitor non-aircraft movement on the AOA as well as along external boundaries of an airport. This concept is illustrated in *Figure III-A-4* and *Figure III-A-5* below.

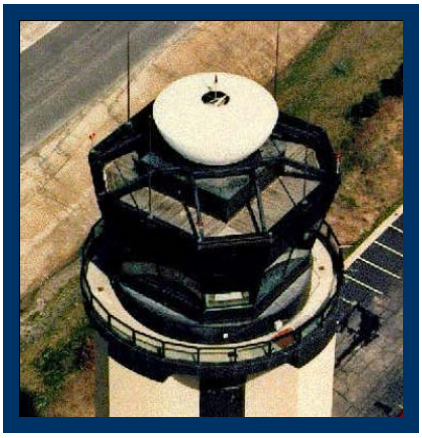


Figure III-A-4 - ASDE Radar

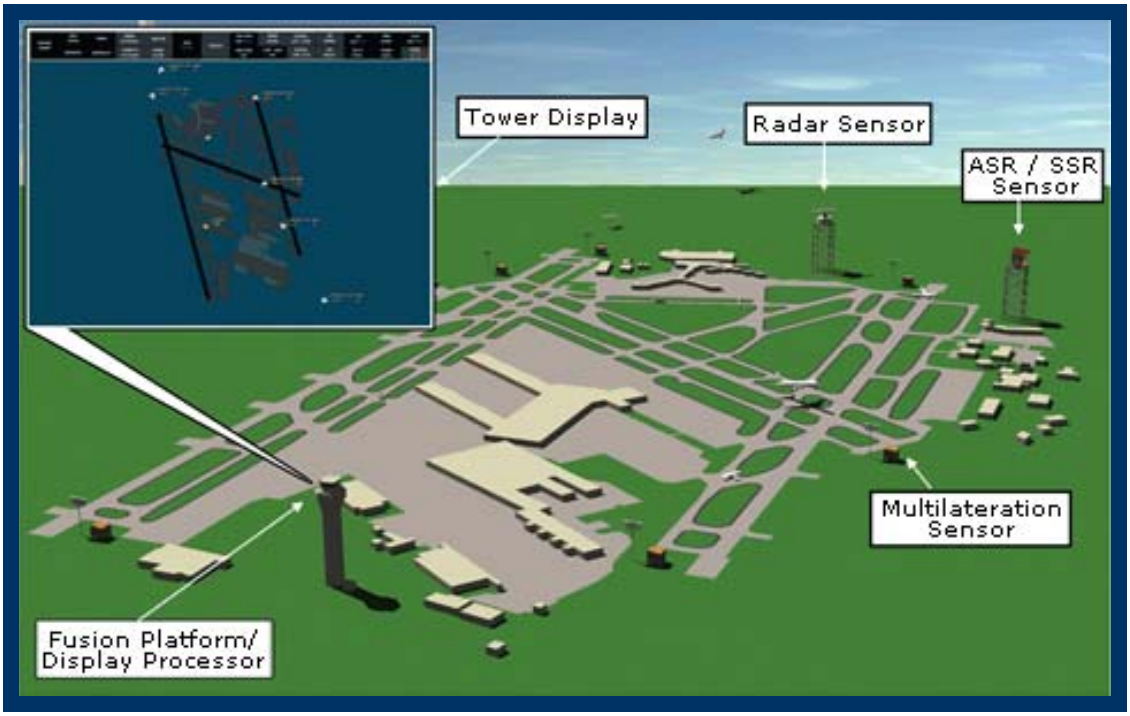


Figure III-A-5 - ASDE Radar & Its Adaptation for Surface Security and Intrusion Detection

Tests by TSA's Transportation Security Laboratory are designed to demonstrate that modified ASDE radar could differentiate between "approved" and "unauthorized" targets, including persons and ground vehicles as well as marine craft approaching a waterside perimeter. The radar is intended to determine the origin and track the paths of movement of these targets. With further development, the system is expected to classify an object, to predict its likely next movements or directions, and to assist the

operator in providing an appropriate level of response. Some of these functions can also be automated and applied to pre-programmed zones of priority to enhance security decision-making.

c. Natural Barriers

The use of natural barriers may be necessary or advantageous 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 in lieu of standard physical barriers or in conjunction with and as a complement to additional security measures or procedures.

Natural barriers may include bodies of water, expanses of trees, swampland, dense foliage areas, cliffs, and other such areas.

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 earthed 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 achieving a visual reference of the airfield. The stockpiling of material can also be used to create a visual barrier, but must not impact any protected surfaces or create an impact to the safe and efficient operation of aircraft or any airport operation. 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 optional natural barrier. This concept suggests that if an unauthorized entry were to occur at a particular location, the amount of time and distance, 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 barriers or boundaries are relatively removed from the critical areas they are protecting.

Another common security design principle is known as “DDR: Detect, Delay, Respond”, in which protection of a relatively remote perimeter or facility may require only moderate security measures if it is sufficiently removed from the primary security-related areas to allow the airport to detect an intrusion, and delay its progress until an appropriate security response can be implemented.

d. Access Points

Typically there are access points through fencing or other barriers for both vehicles and pedestrians. Access points through buildings or walls are typically doors; guard points or electronic means or controls may be also used. 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. So, in all cases, the number of access points should be minimized and their use and conditions closely monitored.

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 operations, maintenance operations, and emergency operations.

a) 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 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, 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. See *Electronic Access Points* on page 31 for further information

b) Maintenance Operations

Maintenance operations gates at an airport are typically those used by the airport, tenant and FAA personnel to perform regular and periodic maintenance to remote grounds or equipment. Typical maintenance tasks include mowing, utility service, navigational and communications equipment maintenance.

These gates, unless high-throughput or jointly used for routine operations, are typically non-automated, non-electronic.

c) Emergency Operations

Emergency operations gates are gates used by on-airport and mutual aid emergency response vehicles responding to emergency situations, especially those involving an aircraft, but may also be used for regular operations

Airport emergency operations gate controls may be controlled from an emergency operations center; or from the ARFF response vehicles themselves.

A 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. Consider special paint markings to identify the frangible fence or gate sections to approaching response vehicles.

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 be securely closed and locked, where enhanced security conditions require it. Swing gate hinges should be of the non-liftoff type or provided with additional welding to prevent the gates from being removed.

Security provided by gates can be improved if they are designed and installed with no more than 4'-6" of ground clearance beneath the gate. Where cantilever (slide) and/or rolling gates are used, consideration should be made during planning and design to curb heights, wheel paths, potential obstructions, local weather/wind phenomena, and drainage issues throughout the full path of the gate and in its 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 which may prolong the efficient operation of a slide gate.

If "tailgating" entry is a concern at un-staffed 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 "vehicle entrapment gate") is one method that could help prevent "tailgate" entry. Such gates are separated 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 have also been used to successfully monitor vehicle movement and assist in detection of "tailgate" entries. "Tailgating" and "reverse tailgating" (where a vehicle enters a gate opened by an exiting vehicle) at automated gates may also be reduced by use of a security equipment layout that provides space for waiting vehicles to stop, which obstructs, or at least deters other vehicles from passing through. 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.

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.

2) Doors

To prevent unauthorized access to the airside, doors leading from unsecured areas of the terminal to the airside, and which 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 best control these doors. It may, however, be preferable to include the

use of electronic control devices, such as CCTV or cardreader/pinpads, 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 essential, these doors 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 security control center. 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 delay egress hardware. Each airport must work with local fire and building code officials to determine the best systems allowable to accommodate both emergency and security needs. See also *Emergency Exits* on page 70 for information regarding NFPA fire codes on emergency exits.

Passenger gates, aircraft loading walkways and other devices used for aircraft loading must be capable of being locked or otherwise secured to prevent unauthorized access to the airside and parked aircraft.

3) Guard Stations

Manned guard stations to control access into a security area may be appropriate at some locations. The purpose of such guard stations is to provide a point of entry at which personal identification can be established and persons and vehicles can be permitted to enter according to local security program requirements which vehicles require search.

a) Devices such as turnstiles, tire shredders, roll gates, pop-up barriers, or a remotely operated drop arm barrier gate may be used at guard stations to impede passage through the guard station until access authority is verified.

b) Use of a sheltered checkpoint station is recommended for gates secured by security personnel. The shelter can be designed to permit maximum visibility over the immediate area of the gate and to provide easy access for the guard to carry out the duties of inspecting vehicles and their contents.

c) 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 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, by agreement between the airport and the TSA. Dependable and instant communications from these stations to a central location must be installed, maintained, and frequently tested.

d) 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.

e) 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 at the Security/Communications Center.

4) Electronic Access Points

a) Automatic Gates

In cases where gates are automated and induction loops are used on the airside of gates for free vehicle exit, ensure the loop is located so as to minimize the possibility of objects being thrown or pushed from the public side to activate the loop. Additional access control measures, such as microwave, infrared or other vehicle sensors or CCTV monitoring may be desirable in addition to loops where space is limited or additional security is desired.

Consider means of protecting access control devices (such as card readers or other monitors) serving exterior vehicle gates to reduce possible physical damage from passing vehicles. Properly placed

curbing, bollards, and highway railing are useful for this purpose. Consider also protection of equipment from weather elements, including protection from 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.

b) Doors with Access Controls

There are numerous technologies available for controlling access through doors (magnetic stripe, Weigand, proximity, Smart card, etc.) and there are numerous ways of implementing their use at any kind of doorway – wooden doors, glass, metal, single or double doors, roll-up doors, or indeed at electronic barriers where there is no physical door at all. The designer should take into account any existing 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 and security management. An extensive discussion of this issue is found in the RTCA document DO-230A, "Standards for Airport Security Access Control Systems." Recent technological advances may provide additional solutions including biometrics.

c) 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 electronic sensor technology used (see *Electronic Boundaries* on page 27 for further information), sensor line gates may be comparable in cost to mechanical ones.

The use of sensor line gates is typically the most 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.

d) Automated Portals

Automated access portals are designed for high-throughput, performing access control and/or providing sensing technology in a high-speed, multi-user fashion, yet also providing a positive means of access denial of unauthorized persons. They typically provide an unobstructed pathway 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 additional explosives, drug, or weapon sensing technology to high-throughput areas.

There are also portals and sensing technologies under development that are sensitive to the direction of the intruder's movement, and automatically provide photographs of security violators, and/or detain unauthorized individuals. As technology advances, the capability and affordability of automatic portals will increase and should be evaluated for high-throughput and/or special-use access point locations.

5) Vehicle Inspection Stations, Blast Protection, and Road Barriers

Manned vehicle inspection stations and vehicle crash barriers in roadways may be necessary to control access in and around the airport terminal and other airport facilities. Additional, non-permanent measures may also be necessary during elevated threat levels or 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 access roadway. Vehicle inspection stations may also be necessary at vehicle parking locations that are located within the blast envelope. Consideration should be given to including the following features at vehicle inspection stations.

a) Turnstiles, roll gates, or vehicular crash barriers should be provided that will stop or impede "gate crashing."

b) 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.

c) Sufficient space should be considered to direct a person or vehicle to one side for further inspection without blocking access for those following. Dependable and instant communications from these stations to the Security Operations Center (SOC) or other appropriate central location should be installed, maintained, and frequently tested. Sufficient space should be provided for emergency vehicles and other pre-authorized vehicles to by pass the vehicle inspection stations to access the terminal.

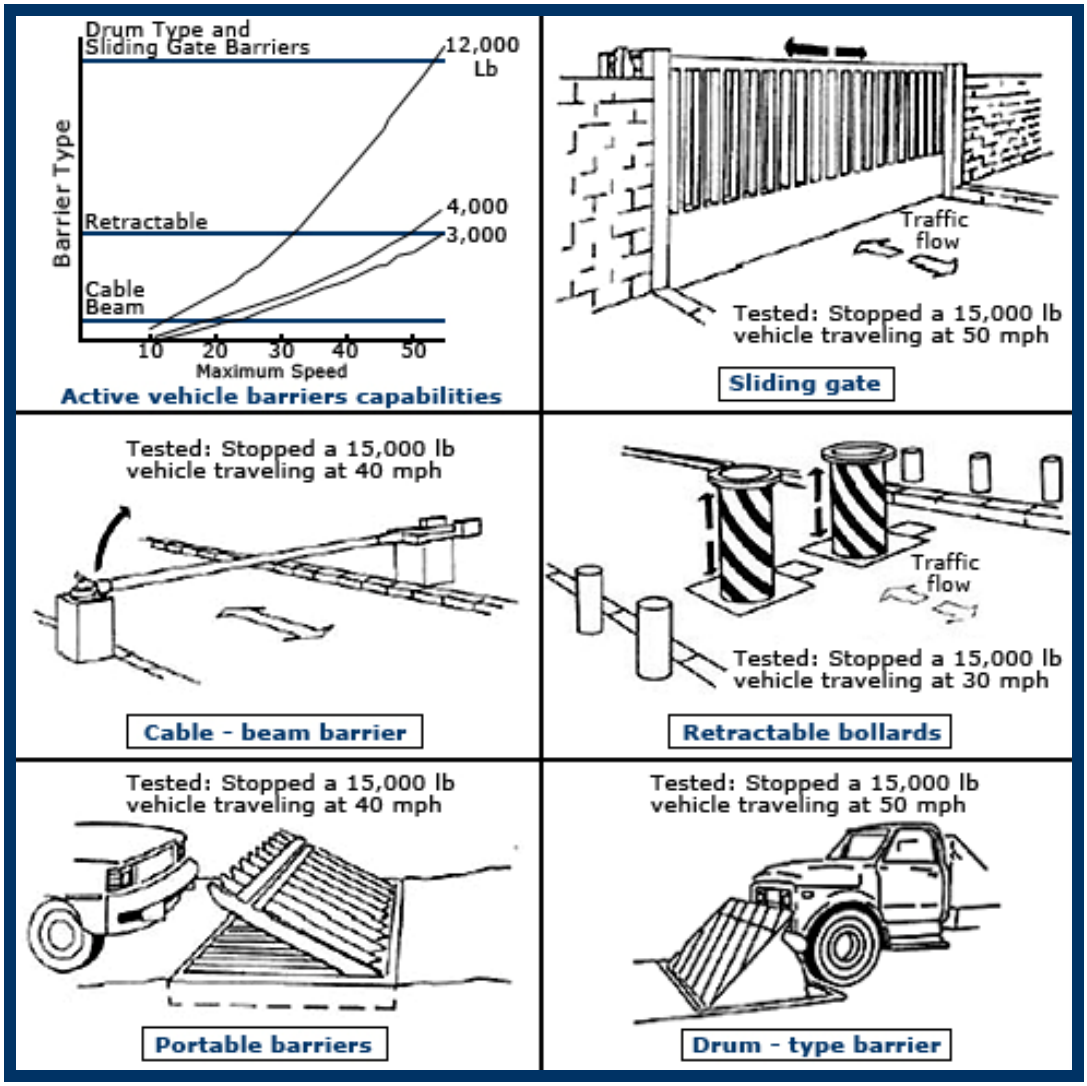
d) A duress alarm system should be provided.

e) Provide ample vehicle queuing distance and vehicle inspection portals to avoid long traffic backups and delays.

Airports are faced with the possibility of attack by explosive-laden vehicles. Fortunately, there is a considerable body of knowledge on blast effects and protective measures available at U.S. government laboratories and agencies. In addition, the U.S. Department of State (DoS) has developed standards for vehicle crash barriers which airport designers can apply with confidence in the level of protection afforded.

Figure III-A-6 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. Barriers should also be designed to work with other measures, such as physical setbacks of buildings and natural barriers such as berms, on developing a blast protection solution.

Figure III-A-6 - Types of Road Barriers



Blast effects and protective measures have been extensively studied and tested. *Table III-A-2* below and *Table III-A-3* on page 36 show the lethal blast radii for various types of threats and the types of blast-protection measures that barriers might be considered to protect against each type of threat.

Table III-A-2 - Lethal Radius of Various Explosive Packages

Type of Expolsive	Expolsive Capacity in TNT Equivalents	Lethal Air Blast Range
Pipe Bomb	5 lbs. (2.3 kg)	
Briefcase, Backpack, or Suitcase Bomb	50 lbs. (23 kg)	
Compact Sedan (in trunk)	500 lbs. (227 kg)	100 ft. (30 m)
Full Size Sedan (in trunk)	1,000 lbs. (454 kg)	125 ft. (38 m)
Passenger or Cargo Van	4,000 lbs. (1,814 kg)	200 ft. (61 m)
Small Box Van (14th ft box)	10,000 lbs. (4,536 kg)	300 ft. (91 m)
Box Van or Water/Fuel Truck	30,000 lbs. (13,608 kg)	450 ft. (137 m)
Semi-trailer	60,000 lbs. (27,216 kg)	600 ft. (183 m)

Source: Transportation Security Working Group,"Terrorist Bomb threat Standoff (Card)," Government Printing Office (1999).

Table III-A-3 - Comparative Effectiveness of Barrier Types

		Vehicle		Protection Level (0-10)
		Weight	Speed	10
Passive Barrier Test Results	Concrete Filled Steel Bollards	4,500	30	1
	Jersey Barrier	4,000	50	2.6
	Straight Retaining Wall	15,000	30	3.6
	Sloped Back Retaining Wall	15,000	40	6.4
	Concrete Planter Retaining Wall	15,000	50	10
Active Barrier Test Results	Cable - Beam Barrier	10,000	15	.6
	Rectractable Bollards	15,000	30	3.6
	Portable Barriers	15,000	40	6.4
	Drum Type Barriers	15,000	50	10
	Sliding Gate	15,000	50	10

Source: Military FM 5-114

DoS performance requirements for vehicle crash barriers are based the kinetic energy represented by the mass of a vehicle and its impact velocity. These "K" ratings are:

K4 15,000 lb vehicle impacting at 30 mph
K8 15,000 lb vehicle impacting at 40 mph
K12 15,000 lb vehicle impacting at 50 mph

To be certified with a Department of State "K" rating, a barrier must demonstrate the ability to stop a 15,000 vehicle and the bed of the vehicle must not penetrate the barrier by more than 36 inches. Additional information on DoS security measures can be obtained from the Bureau of Diplomatic Security, Physical Security Programs, Physical Security Division (DS/PSP/PSD).

DoS certified barriers can be configured as pop-up wedge type barriers, as illustrated in *Figure III-A-7* below, or as vertical bollards or any other configuration which meets the above performance requirements.

Figure III-A-7 - Example of Pop-Up Wedge Vehicle Crash Barrier

e. Other Security Measures

1) Fence Clear Zones

a) 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 any other critical facilities. Such clearance areas facilitate surveillance and maintenance of fencing and deny cover to vandals, trespassers and contraband.

b) 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, the parking of vehicles along the fence should also be prevented. In addition, landscaping within the clear zone should be minimized or eliminated to reduce potential hidden locations for persons, objects, fence damage, and vandalism.

c) There have been cases in which individuals have gained access to passenger aircraft by scaling or crashing through perimeter fencing. To deter or delay attacks, sufficient distance should be maintained between the perimeter fencing and aircraft parking areas.

2) Security Lighting

Lighting of the area on both sides of gates and selected areas of fencing is highly recommended. Lighting beneficial for security inspection, and to assure that fence/gate signage is readable and 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 in areas which have minimal traffic throughput in the off-peak hours.

3) Locks

Advanced electronic 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, particularly those that are

low-risk, low throughput, or significantly distant from the main areas of concern or from the central control station. Note that securing perimeter access portals through the use of locks necessarily involves procedural elements such as a key management system and the 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.

4) CCTV Coverage
   a) While gates, like all other access points, should be kept to a minimum and, where physically and economically feasible, should be considered for treatment with access control and CCTV monitoring, it is recognized that certain low-traffic gates, maintenance access points and gates well removed from the principal areas of security concern may be candidates for greater reliance on time-and-distance considerations.
   b) Further information on CCTV Systems and coverage is contained in *Surveillance and Video Detection Systems* on page 162.

5) Signage
   a) TSA requires signage on certain security boundaries and access points. Specific requirements are found in the ASP pursuant to 1542.201 (secured area) and 1542.203 (AOA). Signs should be located such that when standing at one sign, the observer should be able to see the next sign in both directions.
   b) The use of signage, even in some non-required locations, provides a deterrent by calling attention to the boundary and stating the consequences of violating.
   c) Many locations with access control or surveillance equipment such as CCTV may warrant signage for either directional or legal purposes (e.g. “Alarm will sound if opened”, “Authorized personnel only”, “Notice: All activities in this area are being recorded via CCTV”, etc.)
   d) While signage for security purposes should be designed to draw attention, it should be coordinated with the airport for policy, style and consistency. Based on local environment, the use of multi-lingual security signage should also be considered.
   e) Refer to the *Terminal Section* on page 58 for additional signage information.

Section III-A-5 - Boundaries & Access Points Checklist:

- ☐ **Boundary Choice Factors**
  - Equipment Cost
  - Installation Cost
  - Maintenance Cost
  - Effectiveness
  - Functionality
- ☐ **Physical Barriers**
  - Align with security area boundaries
  - Fencing
    - Select fencing type based on threat and vulnerability assessments, aesthetic considerations, and cost
    - Typically 7' chain link fabric + 1' barbed wire
    - Fence designs are available which are difficult to climb or cut
    - Select barrier types based on threat and vulnerability assessments, aesthetic considerations, and cost
      - Permanent barriers
      - Movable barriers
      - Bollards
      - Vehicle crash barriers
    - Motion, tension or other electronic sensing means available
    - Allow access points for vehicles and persons
    - In critical areas, anchor or bury the fence bottom
    - Keep lines straight and noncomplex
    - FAA References include:
      - Advisory Circular 150/5360-13
      - Advisory Circular 150/5370-10
      - 49 CFR 1542.201 & 1542.203
  - Buildings
    - May be used as a physical barrier
    - May be incorporated into a fence line
    - Assess security access points
  - Interior Walls
    - Security walls should be full height, floor-to-solid ceiling or to slab
  - Exterior Walls
    - Aesthetic designs available
    - Minimize hand & foot holds that can be used for climbing
    - Consider topping walls with barbed wire or other deterrent materials
- ☐ **Electronic Boundaries**
  - Electronic sensors
  - Motion detectors
  - Infrared sensors
  - Stand-alone or used with other barriers
- ☐ **Natural Barriers**
  - Bodies of water
  - Expanses of trees
  - Swampland
  - Dense foliage
  - Cliffs
  - Other areas difficult to traverse
  - Natural barriers may provide "time and distance" protection
- ☐ **Access Points**
  - Minimize the number of access points
  - Gates
    - Plan for routine, maintenance, and emergency operations:
      - Patrols
      - Emergency Response Teams
      - Service Vehicles and Tugs
      - Delivery Vehicles

        - Maintenance Vehicles
    - Design for high activity/long gate life
    - Gate hinges should be non-liftoff or have welding to prevent removal
    - Automate/Monitor gates as necessary
    - Reduce ground clearance beneath, typically to no more than 4-6 inches
    - Two-gate systems can help prevent “tailgate” entry (sally ports)
    - FAA References include:
        - Advisory Circular 150/5300-13
        - Advisory Circular 150/5360-9
        - Advisory Circular 150/5360-13
        - Advisory Circular 150/5370-10
- Doors
    - Avoid unsupervised emergency exit doors to the AOA
    - Automate/Monitor doors as necessary
    - Coordinate hardware with building and fire codes
- Guard Stations
    - Manned access control and search capability
    - Size number of inspection lanes against predicted traffic volumes and inspection processing rates
    - Vehicle lane widths and heights should be matched to largest vehicle accessing the airport
    - Provide sheltered checkpoint station
    - Provide adequate secondary inspection space
    - Dependable communications required
- Electronic Access Points
    - Automatic Gates
        - Locate induction loop to minimize objects from the public-side activating loop
        - Consider bollards to reduce equipment damage by vehicles
        - Protect of electronic equipment from weather and temperature
    - Doors with Access Controls
        - Numerous technologies available
        - See RTCA DO-230A, “Standards for Airport Security Access Control Systems”
    - Sensor Line Gates
        - Function as access-controlled gates
        - Reduced delay time for access
        - Higher risk due to lack of barrier
    - Automated Portals
        - Designed for high-throughput
        - Can include screening technologies
        - Direction sensitive capabilities
        - Can detain violators
- Other Security Measures
    - Fencing Clear Zones
        - Both sides of fence
        - No obstructions
        - Minimal landscape
        - No climbable objects
    - Security Lighting
        - Both sides of gates and fencing is highly recommended
    - Locks
        - Various key technologies available
        - Consider total life cycle costs, not just initial capital cost
    - CCTV Coverage
        - CCTV can be used to enhance detection and/or response
    - Signage
        - Specific requirements are in ASP
        - TSA/FAA-required signage per Advisory Circular 150/5360-12C
        - Deterrent signage
        - Instructional and/or legal signage
        - Coordinate with airport signage policy

6. Facilities, Areas and Geographical Placement

When determining the security requirements of all airport facilities, examine the interaction and relationships among the various areas, the types of activity within each area, the flow of public and employee traffic to and through each area, the flow and type of delivery and maintenance traffic, potential needs for and frequency of security escorts, and the manner in which each such area is addressed in the airport's ASP. A facility's placement in relation to the airside/landside boundary, commercial passenger terminal, and regulated security areas will heavily affect what security and access control requirements exist and who has responsibility for security.

a. Aircraft Maintenance Facilities

Aircraft maintenance facilities may be completely landside, completely airside or part of the airside/landside boundary line. As these facilities contain aircraft ramp and/or hangar areas as well as involve public access and supply delivery, their property and/or buildings are typically parts of the airside/landside boundary line and as such 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
- Prevention of unauthorized access to and 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

b. Aircraft Movement Areas

By definition, aircraft movement areas (runways, taxiways, aircraft ramps) are completely airside, are required to be within the AOA or secured area, and require security measures per 49 CFR 1542 as well as adherence to appropriate Federal Aviation Regulations (FARs).

Detailed information is contained in *Aircraft Movement Areas* on page 47 under the *Airside* section.

c. Aircraft Rescue and Fire Fighting (ARFF) Facilities

ARFF stations and their equipment are a requirement of 14 CFR 139, Subpart D, Certification and Operations: Land Airports Serving Certain Air Carriers, which is administered by FAA. These facilities are clearly critical to an airport's operations. Typically, even in a multi-station scenario, 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).

Positioning of each ARFF station must consider emergency response times and routes. Thus, stations are located for minimum response times to 14 CFR 139 required locations. ARFF vehicles may need landside access for response to landside incidents.

ARFF stations generally include a training classroom that is often used for training airport tenant employees and related activities. If possible, portions of the ARFF station should be accessible without requiring persons to pass though access controls. However, other portions of the ARFF station must be controlled to prevent unauthorized access to the airside.

Similarly, the administrative office area of an ARFF station may be open to public access, enabling persons having business with ARFF officers to access these areas without access control.

In all cases listed for this section, coordinate ARFF facilities with airport staff to determine design direction and resulting operations.

d. Security Operations Center (SOC)/Airport Emergency Command Post (CP)

The title for locations where an airport operates from during normal security operations, as well as during an emergency, event or incident varies by individual airport. Typical titles for facilities where normal security dispatch and operations occur include Security Operations Center (SOC) and Airport Operations Center (AOC). Typical titles for facilities where airport emergency operations occur include Airport Emergency Command Post (CP) and Airport Emergency Operations Center (EOC). For purposes of this document, the standardized terminology SOC and CP shall be used.

When addressing SOC and CP facilities, it should be noted that demand for their use may be for a single or potentially, multiple events happening concurrently. It may also be necessary to address redundant systems, or at least redundancy of primary components installed in a SOC and/or CP, for location in other areas of the airport is it within a terminal or an alternate facility. In addition, links to other government emergency facilities may enhance the operation of an airport's CP.

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 secure area. The designer must be certain to 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. 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 to 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 such public-related systems and services such as paging, lost and found, or first aid.

For a full discussion on these areas and their contents, see *Security Operations Center* on page 78 and *Airport Emergency Command Post* on page 79 under the *Terminal* section.

e. Airport Personnel Offices

Most personnel and administrative offices typically 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. In addition, some personnel offices, such as airfield maintenance or operations, may be completely airside.

Most airport personnel offices are located in or near the terminal, and are secured (nonpublic) at least part of the time. See *Airport Personnel Offices* on page 76 under the *Terminal Nonpublic Areas* section.

f. Belly Cargo Facility

Belly cargo is carried on passenger aircraft rather than all-cargo or freighter aircraft. Belly cargo facilities share many of the same security requirements as standard cargo areas, and in many airports may be part of one joint cargo facility or area. However, some airports maintain a completely separate area for belly cargo that will be traveling in passenger aircraft rather than cargo planes. One of the primary differences between most dedicated belly cargo facilities and other cargo facilities is that the belly cargo facility may not need to be attached to or adjacent to an aircraft ramp. Since most belly cargo is handled via tugs, a belly cargo facility can be located either adjacent to the terminal where its aircraft operator aircraft are, or at any point along a service roadway which connects to the terminal. A standard cargo facility on the other hand may need to handle aircraft cargo directly where the plane actually pulls up to a fixed or movable loading bridge.

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 a belly cargo facility to be designed with potentially higher or stricter security levels. Since belly cargo usually involves smaller quantities of public air cargo and U.S. mail, belly cargo facilities can be designed which have the potential for 100% Explosives Detection System (EDS) 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. Refer to the *Security Screening* section on page 87 for further information.

A facility for shared cargo screening, including belly cargo and regular cargo, should be considered.

g. 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 roads associated therewith.

Refer to the *Security Screening* section on page 87 for further information.

h. FAA Airport Traffic Control Tower (ATCT) and Offices

The FAA ATCT and its administrative offices may be located within or adjacent to a terminal complex or in an airside or landside area. ATCT location is dependent upon runway configuration and line of site criteria. ATCT security needs should be addressed by the airport planner and designer such that an interface takes place with FAA security requirements for FAA ATCT design criteria. When the ATCT is in a remote airport location, it may require significant levels of protection as one of an airport's most critical operational facilities. Coordination with the FAA, TSA and the airport is necessary in order to address all ATCT security impacts or requirements to airport operations.

i. 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 and require attention. Security fences should surround the fuel 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. Closed circuit television monitoring, alarms and sensing should be considered in and around fuel farms and storage tanks to alert law enforcement/security personnel of potential intruders or tampering.

j. General Aviation (GA) and Fixed Base Operator (FBO) Areas

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

For information on security at non-commercial general aviation airports, see TSA Information Publication (IP) A-001, "Security Guidelines for General Aviation Airports", issued in May 2004. The TSA document is available on the Internet at

http://www.tsa.gov/interweb/assetlibrary/security_guidelines_for_general_aviation_airports_may_2004_a-001.pdf

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

Further information is in *General Aviation (GA) Parking Area* on page 47 under the *Airside* section.

k. Ground Service Equipment Maintenance (GSEM) Facility

Many airports today 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 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 travel.

As with other service and maintenance areas, particular attention should be paid to material and vehicle parking/storage areas and assuring they do not compromise airside fencing clear zones or security.

l. Ground Transportation Staging Area (GTSA)

A GTSA is a designated area where taxis, limos, buses and other ground transportation vehicles are staged prior to the terminal. By nature, these areas are always landside as it involves public and private off-airport transportation services.

Refer to the *Ground Transportation Staging Area (GTSA)* section on page 52 under *Landside* Facilities.

m. Hotels and On-Airport Accommodations

By nature, hotels and on-airport accommodations are always landside as they are public facilities.

Refer to the *Hotel and On-Airport Accommodations* above under *Landside* Facilities.

n. Industrial/Technology Parks

Industrial/technology Parks may be landside, airside or both. Many airports have land available or in use as industrial/technology parks. Evaluate this land use for security impacts to the airport's operations.

o. 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 needs and choices may require substantial amounts of coordination, both architecturally and procedurally. Determination of the security risk involving catering operations should be evaluated in advance of design or construction of these facilities.

p. Intermodal Transportation Area

While *intermodal* transportation areas vary greatly in function and location, they are typically always completely landside facilities. The function of an intermodal transportation area is to transfer passengers or cargo from one mode of transportation to another (i.e., train to plane, bus to plane).

Detailed information is contained in Intermodal Transportation Areas under Landside Facilities.

q. Isolated Security Aircraft Parking Position

The Isolated Security Aircraft Parking Position is a location within the airside 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.

Detailed information is contained in *Isolated Security Aircraft Parking Position* on page 48 within the *Airside* section.

r. Military Facilities

Some airports may have adjacent or on-airport military facilities such as Reserve, National Guard or active duty units. Since each of these situations is unique, and since these facilities may be partially airside, or adjacent; detailed coordination between the airport, FAA, TSA, and the military facility must occur for both design and procedure. Typical areas of coordination include access control, identification 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 assure 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 4-010-01 for Department of Defense (DOD) Minimum Anti-Terrorism Standards for buildings used by the military.

s. Navigational & Communications Equipment

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

t. Passenger Aircraft Loading/Unloading Parking Areas

Passenger aircraft loading/unloading parking areas are required to be airside and are typically at or near the passenger terminal, are required to be within the secured area, and require security measures per 49 CFR 1542.

Detailed information is contained in Passenger Aircraft Loading/Unloading Parking Areas within Airside.

u. Passenger Aircraft Overnight Parking Areas

Passenger aircraft overnight parking areas are required to be airside and are typically adjacent to the passenger terminal, but may also normally be on a designated ramp located remotely from the terminal. These areas are required to be within the AOA or secured area, and require security measures per 49 CFR 1542.

Detailed information is contained in Passenger Aircraft Overnight Parking Areas within Airside.

v. Rental Car and Vehicle Storage Facilities

Rental car facilities and vehicle storage are usually landside.

See the *Rental Car Storage Areas* section on page 52 under *Landside* Facilities.

w. 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/Fixed Base Operator (FBO) areas. However, because of their nature, non-military government aircraft support facilities are typically 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.

x. 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 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.

Detailed information is contained in Terminal Patron Parking Areas within Landside.

y. 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 identification media issuance and access may require utilities to be landside. Special emphasis should be given to aboveground electrical substations.

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 area, security treatments such as bars, grates, padlock, 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.

Section III-A-6 - Facilities, Areas and Geographical Placement Checklist

☐ **Facility Placement Considerations:**
- Interaction and relationships among areas
- Types of activity within each area
- Flow of public/employees to/through areas
- Flow and type of delivery traffic
- Flow and type of maintenance traffic
- Need for and frequency of security escorts
- How each area is addressed in the ASP

☐ **Each Airport is Unique**

☐ **Facilities:**
- Aircraft Maintenance Facilities
  - Airside, Landside or Both
  - Security the responsibility of the facility
- Aircraft Movement Areas
  - Airside
  - Requires controlled access
- Passenger Aircraft Overnight Parking Area
  - Airside
  - Requires controlled access
- ARFF Facilities
  - Either Airside or Both
  - Consider response routes and times
  - Facility may require public access
- SOC/CP
  - Secure location
  - Consider alternate/back-up locations
  - Ease of airside access
  - Sufficient operating space for personnel
  - Central location for dispatching
  - See Terminal Nonpublic Areas Checklist
- Airport Personnel Offices
  - Airside, Landside or Both
  - Consider security needs
  - See Terminal Nonpublic Areas Checklist
- Belly Cargo Facility
  - Airside, Landside or Both
  - Flexible Placement
  - Terminal Access (via roads) required
  - Consider cargo screening needs
- Cargo Area
  - Typically Airside or Both
  - Screening and inspection needs
  - Secure cargo-holding area
  - Postal facility inclusion possible
  - Doors must be lockable and controlled
  - Consider fence protection measures
- FAA ATCT and Offices
  - Landside or Airside
  - May require airport security controls
- Fuel Area
  - Landside or Airside
  - Typically remote from terminal
  - Safety and security fencing required
  - Consider access controls to area
- GA Areas
  - Typically Airside on Both
  - Boundaries based on function
- GSEM Facility
  - Landside or Airside
  - Consider airside travel frequency
  - Maintain fencing clear zones
- GTSA
  - Landside
  - Public Safety and Security Concerns
- Hotels and On-Airport Accommodations
  - Landside
  - Public Safety and Security Concerns
- Industrial/Technology Parks
  - Landside, Airside or Both
- In-Flight Catering Facility
  - Landside, Airside or Both
  - Typically adjacent to terminal
- Intermodal Transportation Area
  - Typically Landside
- Military Facilities
  - Substantial coordination required
- Navigation and Communications Equipment
  - Airside and Landside
  - Driven by functionality
  - Control access to critical equipment
- Rental Car Facilities
  - Landside
  - Public Safety and Security Concerns
- State/Government Aircraft Facilities
  - Both airside and landside
  - Security typically independent
  - Coordinate security requirements
- Utilities and Related Equipment
  - Locate airside when possible
  - Control access
  - Secure access points and equipment

Section B - Airside

The Airside area of an airport involves a complex and integrated system of pavements (runways, taxiways, 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. It is important for planners and designers to evaluate the effective integration of facilities located on the airside as well as use the terrain and/or adjacent land or bodies of water to enhance overall security. The responsibility for Airside security may rest with the airport owner or be delegated to a tenant operating on the airside or under a joint use agreement. Areas and functions which should be included in an airport's security plan include:

1. Aircraft Movement & Parking Areas (Ref. 14 CFR 139)

While the location of aircraft movement and parking areas is typically dictated by topography and operational considerations, the placement of the airside/landside boundary and the respective security boundaries must be 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.

a. Aircraft Movement Areas

Normal aircraft movement areas include all runways, taxiways, ramps and/or aprons. While there are no specific security requirements that 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 (See A/C 150/5300-13), they all share the same types of requirements noted below. While these are not security related areas, their location, orientation and boundaries may have security implications (i.e., 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 AC 150/5300-13.

b. 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; thrown objects, etc.; and visibility of the areas around the parked aircraft to monitor for unauthorized activity. Airports might want to consider including this area as part of the airport's Security Identification Display Area (SIDA).

c. Passenger Aircraft Overnight Parking Areas

Passenger aircraft overnight parking areas are generally the same, or not far removed from, the arrival and departure gates. Where an aircraft must be moved for some 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 aircraft such overnight parking areas are relatively remote, they should monitored and be well lighted, with no visual obstructions.

d. General Aviation (GA) Parking Area

It is advisable, to the extent possible, to exclude separate general aviation areas from the SIDA of the airport. However, this is not always possible, as in the case where international general aviation flights, which would include charters, private and corporate flights, must be directed to the International Arrivals Building area, (IAB) which is almost always found within or attached to the secured area at the main terminal complex. The limited security resources of an airport operator should be focused on the critical passenger aircraft operator areas.

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

General aviation tenants should always be a part of the planning process for security related matters that may affect their operations.

e. Isolated/Security Parking Position

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 remove and examine cargo, mail and stores removed from an aircraft during bomb threat conditions, and 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 "hot spot" in many Airport Security Programs. 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. (Reference See ICAO Annex 17).

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 meters) from other aircraft parking positions, buildings, or public areas and the airport fence. ICAO Annex 14 advises the allowance of at least 328 feet or 100 meters. 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, aviation fuel, water mains, or electrical or communications cables.

Isolated aircraft parking areas would ideally be located to eliminate the possibility of unauthorized access to, or attack on, persons physically reaching or being able to launch an attack against the aircraft. Consideration should be given to the parking area's visibility to 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.

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. The area's capability for cellular, radio and other wired or wireless methods of communication should also be considered.

2. Airside Roads

Roads located on the airside should be for the exclusive use of authorized persons and vehicles. Placement and quantity of airside roads should not only consider standard operational and maintenance needs, but also emergency response needs and access to crash sites and isolation areas. 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 fences should be established.

3. Airside Vulnerable Areas & Protection

The airport designer, in concert with security and operations leadership, must consider such things as NAVAIDS, runway lighting and communications equipment, fueling facilities, and 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.

4. Airside Cargo Areas

To the extent possible, air cargo facilities should be significantly separated from critical passenger loading areas and general aviation areas. In order to enhance security, airports may consider designating the ramp area adjacent to their air cargo facilities as a SIDA area. Taxiways leading to the cargo areas, if possible, should be planned to avoid ramps used by commercial passenger aircraft operators. Additional information on cargo security requirements is found in the *Cargo Screening Section* on page 148.

Section III-B - Airside Checklist:

- ☐ **To support aircraft operations, ramp areas should be securable**
- ☐ **Factors influencing boundary locations:**
  - Aircraft Movement Areas
    - Runways, taxiways, ramps and/or aprons (See A/C 150/5300-13)
    - FAA safety and operational areas (See 14 CFR 77)
      - Object Free Area
      - Building Restriction Lines
      - Runway Protection Zone
      - Runway Safety Area
      - Glide Slope Critical Area
      - Localizer Critical Area
      - Approach Lighting System
  - Passenger Aircraft Parking Areas
    - Safe distance to fence/public access areas
    - Safe distance to other parked aircraft
    - Safe distance recommendations for prevention of vandalism
    - Maintain visibility of areas around parked aircraft to monitor for unauthorized activity
  - General Aviation (GA) Parking Area
    - Exclude GA from the SIDA
    - Distance GA from terminal area
    - Coordinate with tenants
  - Isolated/Security Parking Position (See ICAO Standards Annex 14 & 17)
    - At least 100 meters from other aircraft and structures
    - Ensure separation from utilities and fuel
    - Use CCTV to view the aircraft and surrounding area
    - Accommodate emergency staging area
    - Avoid public viewing/proximity to area
- ☐ **Airside Roads**
  - Restrict access to authorized vehicles
  - Perimeter roads should be airside
  - Perimeter roads should provide unobstructed 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 ATCT

Section C - Landside

Landside – The landside of an airport is that area of an airport and buildings to which both traveling passengers and the non-traveling public has unrestricted access. Samples of facilities located within the landside are: public and employee parking, terminal and public roadways, rental car and ground transportation operations, hotel facilities, commercial and industrial developments.

Security in the landside area 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 obstacles to overcome 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 remain as vulnerable targets and yet basic tenets of physical security are 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.

1. Natural Barriers

The use of natural barriers in the airport landside area may be necessary or 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 lieu of standard physical barriers or in conjunction with and as a complement to additional security measures or procedures.

Refer to *Natural Barriers* on page 29 for a description of possible natural barriers.

2. Landside Roads

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

When planning landside roads, bear in mind their proximity to security fencing, considerations of potential airside access where elevated roadways may provide access or threat to adjacent areas of the terminal, or apron and/or nearby aircraft. When security levels are raised, consider the method and location for performing vehicle inspections outside of the "blast envelope" established in the Blast Analysis Plan (BAP) for the terminal. This can be accomplished with temporary or permanent inspection stations positioned on the approach roads. Vehicle inspection stations should possibly include conduit and rough-ins at those locations for power, communications and security data lines.

a. Vehicle Inspection Stations

Manned vehicle inspection stations to control access in and around the airport terminal during elevated threat levels are necessary at most airports to provide a location outside of the "blast envelope" in which to inspect vehicles that are approaching the airport terminal on the access roadway. In some instances, vehicle inspection stations are also necessary at vehicle parking locations if they are located within the blast envelope. Consideration should be given to including the following features at vehicle inspection stations:

Turnstiles, roll gates, or vehicular crash barriers that will stop or impede "gate crashing".

A sheltered checkpoint station, if appropriate, is recommended to permit maximum visibility over the immediate area of the gate and to provide easy access for the guard to carry out inspecting duties. A sheltered checkpoint station could be a portable unit.

Sufficient space should be provided to direct a person or vehicle to one side for further inspection without blocking access for those following. Sufficient space should also be provided for emergency vehicles and other pre-authorized vehicles to by-pass the vehicle inspection stations.

It is essential to provide communications, including emergency and duress alarms, 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.

Provide ample vehicle queuing distance and vehicle inspection portals to avoid long traffic backups and delays.

b. Roadway Design

Roads to the terminal should allow for un-congested flow during peak hours so as to ensure law enforcement personnel have the ability to effectively monitor and move vehicles.

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. Consider the use of moving sidewalks or access to luggage carts to help passengers bridge the gap.

Provide for Emergency Vehicle (Fire and Police) Parking / staging areas near the terminal, potential inspection areas, and congested areas.

During periods of heightened security, ensure vehicles cannot gain access to the terminal by bypassing inspection area. Be sure to evaluate the ability of the potential to "jump curbs", travel across open landscaping, or drive the wrong way down a road.

Minimize traffic to the terminal by offering alternative routes to non-terminal based operations, such as access to the Air Cargo operations, Rental Car agencies, hotels, etc.

Clearly sign and allow for sufficient weaving zones to permit drivers unfamiliar with the airport to find their destinations quickly and easily. During periods of heightened security, allow exit points or alternate routes prior to security check points so customers may choose other options or means to access the terminal (such as buses or walking). This will help alleviate some of the congestion and inspection requirements.

3. Landside Parking

a. Terminal Patron Parking

1) 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 injury or damage from a vehicle bomb. Consider allowing a safe distance outside of the established "blast envelope" between parking lots and access roadways to the terminal.

2) Parking area entrances and exits should not be placed in front of or near the terminal. Elevated security levels may require vehicle inspections. Allowing vehicles to go straight into parking areas may alleviate the number of vehicles the inspectors must examine.

3) 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, or closing parking areas off, or segmenting them to control access only by authorized personnel such as employees or other known entities.

a) Parking areas can be sectioned by a variety of mechanical devices. A common method involves the use of "head knockers". These devices limit the height of vehicles that can park in a certain area by suspending an immobile steel bar at the limiting level. Those cars smaller than the bar can then proceed unhindered.

NOTE: Emergency Responders must be made aware of these limitations, and appropriate access points must be established for their needs.

b) Ensure that restricted parking areas cannot be accessed by curb jumping or entry through the exit lanes. Fencing, bollards, or landscaping can often provide the security required.

4) Provide sufficient space in parking areas to facilitate the movement of police, fire and emergency vehicles.

5) 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, and thus the potential for CCTV, lighting, intercoms, and duress buttons to be integrated with the main airport security system.

b. Employee Parking

Protection of employee parking areas, and the employees who use them, is no less important than that of parking areas for the traveling public, and should he treated similarly, especially where they are either remotely located or accessible 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.

4. Landside Facilities

a. Ground Transportation Staging Area (GTSA)

GTSAs may present security and safety concerns, and should be addressed in the planning and design phases. The U.S. Department of Transportation 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, U.S. Department of Transportation, November 2004, contains much useful information for airport planners and designers. The DOT document is available on the Internet at

http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/DesignConsiderations/default.asp

b. 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 include 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 the security point of view, considering potential trajectories from a close-in, publicly accessible, private hotel room. Other considerations include security design elements to accommodate the hotel's cash-handling activities and vendor/supplier traffic at all hours of the day.

c. 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. Typically, light rail or heavy rail systems are being used to bring travelers to the airport, with automated people movers acting as circulators with a connection to a rail station.

When planning, designing or renovating an airport, alternative modes for moving people in and out of an airport must be considered. When such intermodal alternatives are being considered, security and safety concerns must also be part of that consideration. For example, there is a need to provide adequate standoff distance between the transit station and the airport airside to mitigate against use of the transit vehicle as a delivery device for explosives or other weapons.

d. Rental Car and Vehicle Storage Areas

Rental car storage areas are typically 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/or CCTV systems, the considerations for equipment and/or alarm response connections compatible with those of the airport should be made.

Where these areas are located adjacent to security areas or fencing, bollards, curbing or other structures should be planned and designed to prevent vehicles from being parked and stored in locations that would violate the security clear zones. The requirement to maintain this security perimeter may also need to be incorporated into the respective tenant's lease agreement.

5. Entry Control Points (ECPs)

Typically there are access points through fencing or other barriers for both vehicles and pedestrians. Access points through buildings or walls are typically doors. In either case, guard points portals or electronic means or controls may be also used. 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. So, in all cases, the number of access points should be minimized and their use and conditions closely monitored.

ECPs should be sufficiently removed from the terminal and other critical infrastructure such as ATC towers or radar systems, so that vehicle bombs will have minimal affect on critical operations.

a. Gates

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

Routine operations 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.

SIDA, secured area, AOA, and other security boundary gates that are high-throughput are the most likely candidates for automation and electronic access control. Refer to the *Electronic Access Points* on page 31 for further information.

b. Roads

Ensure that roadways accessing entry control points to the Airside of the airport have adequate maneuver room for vehicles using the gate. These points may need temporary staging areas for vehicle inspections that do not hinder traffic flow through the gate.

Access to the ECP 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. Interior Spaces

When interior walls are to be used as security barriers, consideration should be made as to not only the wall type and construction material, but also to the wall's 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 levels of access control to a degree at least equal to that of the rest of the boundary.

7. Exterior Spaces

a. Physical Barriers

Physical barriers can be used to deter and delay the access of unauthorized persons onto 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.

1) Fencing

a) For airports, fencing all or portions of the property involves considerations of the desired level of security (i.e., deterring intrusions or preventing forces 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, aesthetic issues, etc.

b) For fences with sensors, there are other elements to the security system for monitoring of the sensors and response to intrusion alarms. See the *Security Operations Center* section on page 78.

c) Access Points - When utilizing fencing as a security boundary, care must be taken to ensure that the provision of fencing does not conflict with the operational requirements of the airport. Access points will need to be made in the fence to allow the passage of authorized vehicles and persons. While the number of access points should be kept to a minimum, adequate access points must be planned for routine operations, maintenance operations, and emergency operations. For further information on fencing access points see Gates or Guard Stations.

d) Alignment - To assist in surveillance and security patrol inspection, keep fences as straight and uncomplicated as possible, this will also minimize installation and maintenance costs.

e) Clear Zones - 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 any other critical facilities. Such clearance areas facilitate surveillance and maintenance of fencing and deny cover to vandals and trespassers.

   i) 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 other materials. Likewise, the parking of vehicles along the fence should also be prevented. In addition, landscaping within the clear zone should be minimized or eliminated to reduce potential hidden locations for persons, objects, fence damage, and vandalism.

   ii) There have been cases in which individuals have gained access to passenger aircraft by scaling or crashing through perimeter fencing. To deter or delay attacks, sufficient distance should be maintained between the perimeter fencing and aircraft parking areas.

f) Fence Construction - Effectiveness of fencing 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. Mowing strips may also reduce security and maintenance man-hours and costs.

   i) 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.

   ii) 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.

g) Refer to *Fencing* on page 23 for more information on security fencing.

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 be dependent upon the nature of the business being conducted inside, and the level of continuous access required by those personnel.

a) Walls

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

b) Exterior Walls

While not typically 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.

b. Lighting

The use of illumination can help both 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. They 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 the objects in that area which may cast shadows, such as corners, walls, doors, etc. 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.

c. 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 identification media issuance and access may require utilities to be landside, although that must also be secured. Special emphasis should be given to aboveground electrical substations.

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 area, security treatments such as bars, grates, padlock, or other effective means may be required to meet practical maximum opening size requirements. For structures or openings that involve water flow, consider 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 in the security treatment design.

8. Systems and Equipment

a. Electronic Detection and Monitoring

In the case of boundaries which are monitored by electronic sensors, motion detectors, infrared sensors, etc., it is clear that these are intended to serve essentially the same security functions as other detectors, but are simply employing other technologies, usually with somewhat higher maintenance costs. Typically they will 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.

b. 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 subject to federal security regulations, but during implementation of crisis contingency plans they can be expected to be affected by special security measures to prevent criminal acts. Prudent use of surveillance technologies such as CCTV and other technologies should be considered in monitoring areas of concern, in consultation with airport law enforcement, the airport security coordinator, 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.

c. Alarms

Place duress alarms in restroom and/or public areas to reduce facilitate police/emergency response time.

9. Emergency Response

a. Law Enforcement

Provide provisions for a remote police substation or presence in the vicinity.

b. Off-Airport Emergency Response

While first response to many on-airport emergencies, such as fires, medical events or injuries, and traffic accidents, will be by on- airport response personnel, local codes, agreements, or unusual situations may require the response of off- airport emergency or law enforcement personnel. In addition, some airport's primary response personnel (such as for structural fires) may be off-airport organizations, such as Explosives Ordnance Disposal (EOD) units. 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, 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 which can be incorporated into an airport's design include:

1) The use of special "agency-only" identification media, PIN numbers or card readers that provide emergency personnel access without the need to issue identification media to individual persons.

2) Installation of a vehicle ID system, such as radio frequency identification tagging (RFID), that enables emergency vehicles to access security areas and be tracked while on airport property.

3) Incorporation of screening checkpoint "bypass routes" that provide direct sterile area access for escorted personnel and personnel with identification 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.

4) To facilitate quicker response or to keep airport and off-airport emergency personnel advised of incidents, a linked notification system and/or procedure is advised. This will minimize confusion, and 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.

c. Life Safety Equipment

Consider incorporation of life safety (emergency medical) equipment 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. In addition, emergency phones/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.

d. Emergency Service Coordination

It is important to maintain close coordination with the Airport Security Coordinator (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.

e. Threat Containment Units (TCU)

While TCU will typically be stored at some location within the terminal, it is important to determine how the responding bomb squad will gain access to the TCU. The TCU is 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 to maneuver on. Designers should create appropriate TCU access.

Section III-C - 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 AOA/security fencing
  - Pre-terminal screening capability
  - CCTV monitoring for security/safety
- ☐ **Landside Parking**
  - Terminal Passenger Parking
    - Allow significant distance between parking lots and terminals
    - Consider CCTV, lighting, intercoms, and duress alarms for toll plazas
    - 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 and safety concerns include:
      - Driver safety
      - Deterrence of vandalism, theft or other illegal activity
      - Possibility of terrorist or criminal assault
    - Planning/design measures may include:
      - Limitation of concealed areas and locations
      - Provisions for open stairwells
      - CCTV surveillance of the area
      - Duress alarms in restroom and/or public areas
      - Structural layout that minimizes or distributes congested driver waiting areas
      - Sufficient night lighting
  - Hotels and On-Airport Accommodations
    - Possibly connected to terminal
    - Treated no differently than other commercial areas
    - Limit direct line of sight of aircraft
    - Maximize distance to AOA
  - Intermodal Transportation Area
    - Mass transit and light rail systems may require secured transitions
    - Provide adequate standoff distance between transit station and the AOA
  - Rental Car Storage Areas
    - Protect vehicles and workers
    - Potential tie-in to airport access controls
    - Maintain AOA fencing clear zones
- ☐ **Off-Airport Emergency Response**
  - Consider access routes, methods and needs
  - Design features may include:
    - Special identification media, PIN numbers or card readers for emergency access
    - Emergency Access to terminal areas

Section D - Terminal

1. Terminal Security Architecture

From a security perspective, airport terminals are generally divided into two distinct zones, usually known as "landside" and "airside", with the security systems and procedures serving to transition the passenger from landside security concerns and measures to airside security concerns and measures: a transition from land based transportation systems to air based systems; a transition in the flow and focus of passenger movement; and a transition in the management of airport operations as well as evolving governmental security responsibilities.

This transitional aspect of airport terminal planning and design means the planners must accommodate various activities on both the landside and airside while permitting efficient and secure methods for a 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. Successful planning and design processes include the participation of the airport security committee (if one is in existence), fire protection and law enforcement personnel, aircraft operators, the Transportation Security Administration (TSA), various state and Federal government agencies; tenants on both the airside and landside, and both commercial and private aircraft operators, in developing the appropriate strategies to meet current security requirements and provide the flexibility for future change. This section provides information on many of the concepts and methods involved in security planning and design of terminal building facilities.

a. Functional Areas

The basic functionality of operational areas within airport terminal buildings has not significantly changed in years. While we have found new ways to process passengers and bags, through the evolution of automation and technology, the basic functions remain the same. Things are likely to continue to evolve during the next 3 to 5 years as new technologies are introduced, new regulations are imposed, and airlines modify service levels both up (to accommodate larger aircraft, such as the Airbus A380) and down (to accommodate the continuing proliferation of regional jets). The goal of this section is to assist the airport terminal building designer in understanding the need for flexibility and adaptability in the consideration of 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 security requirements, but also to allowing the next designer an optimal opportunity for upgrades and modifications.

Each airport has a unique road system, architectural design, and structural design. Further, airport architectural, structural, and civil and security systems interact in almost every aspect of facility design. Each airport should tailor its security design solutions to suit its fundamental vulnerabilities and needs. Airport planners, architects, and engineers might choose at their own discretion to incorporate such solutions as:

- 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) at curbside and doorways
- Perimeter columns and beams that are resistant to blast
- Vehicle barriers that prevent LVIEDs from driving close or into the terminal
- Vehicle inspection stations with ample vehicle queuing and standoff distances

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

b. Physical Boundaries

Airport terminals vary in usage and configuration, so the implementation of various security measures could take many forms in response to airport planning and programming 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. Building enclosures and partitioning typically provide most of this separation. Large public assembly facilities such as terminals typically have architectural issues 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 *Airport Layout & Boundaries* on page 13; *Landside* on page 50; *Security Screening* on page 87; *ACAMS* on page 150; and *Video Surveillance* on page 162.

Areas that are unmonitored or accessible to the unscreened public must meet 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 there is more flexibility if there is a means of closure for the entire checkpoint area. In such instances divider walls and railings must 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.

c. Bomb/Blast Analysis Overview

Blast analysis and treatments are addressed at considerably greater length in *Appendix C*. During heightened threat levels, vehicle access and parking near the terminal is limited and vehicle inspections are often implemented. To justify driving or parking close to the terminal, a Blast Analysis Plan (BAP) can be developed at the direction of the airport operator.

Bomb/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 as well as 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 usually much lower than when these are implemented as a retrofit.

The primary objective for developing a BAP 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 Large Vehicle Improvised Explosive Device (LVIED), the performance objective is “collapse prevention” and the solution may be to provide blast resistant columns along the curbside of the terminal building. Clearly this is not the only viable solution; each airport must choose the approach they believe is best for their respective facilities.

Priority should be given to implementing blast protection measures that:

- Are passive (do not rely on personnel)
- Augment airport operations and functions
- Consist of durable materials (will not fade, discolor, or become brittle with time)
- Enhance terminal architecture and aesthetics
- Provide cost effective overall security solutions
- Provide measurably improved blast protection

Airport blast protection measures can be separated into two basic categories:

- Structural - These are blast protection measures that can be employed to reduce the blast envelope around the terminal or reduce the need for vehicle inspections. Blast hardening the perimeter columns of the terminal would be an example of this type of feature.
- Non-structural – These are blast resistance 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 windows or trash containers would be examples of this type of feature.

In lieu of incorporating blast resistant solutions in the terminal design, as mentioned above, airports may elect to inspect vehicles that are approaching or parking near the terminal. A "vehicle inspection" methodology is generally acceptable and viable when heightened threat levels occur. However, this labor-intensive solution tends to be more appropriate for 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 functional drawbacks, such as delay and traffic congestion, high inspection 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 LVIED and the terminal building. While parking above, below, and directly adjacent to the airport terminal building offers great convenience for passengers, these 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. However, one should compare the cost of this type of retrofit against the life-cycle cost of a long-term vehicle inspection solution.

d. Limited Concealment Areas/Structures

This topic has been touched on previously under *Public Areas*. Wall configurations, built-in fixtures, freestanding elements, and furnishings should be designed to deter the concealment of parcels containing explosives or other dangerous devices. This is particularly applicable to public areas, such as ticket counters, lobbies, 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 of necessity, such as restrooms, should also be designed to minimize the ability to conceal dangerous devices.

Where structures with concealable areas are unavoidable, consider designs that are easily, quickly and safely searchable. Coordinate furnishings and structure design with local security, search, and threat response agencies to assure the design meets their requirements and needs. Reduced search times can minimize airport downtime, passenger inconvenience, and negative publicity.

e. Operational Pathways

Efficient terminal facilities do much more than move persons and baggage through various spaces. A tremendous amount of 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 preclude 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 must 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 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 to 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. 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 to public areas. Automatic exits to aircraft operations areas (AOA) should be avoided where possible. Elevators have very similar issues. Public elevators should not cross levels of security, although service elevators typically access all levels.

Airport police and other law enforcement entities often need secure nonpublic corridors. LEOs must escort persons from aircraft or various public areas of the building to the terminal police holding areas. This transport or escorting of persons should be along nonpublic corridors. 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.

f. Minimal Number of Security Portals

Architecture should be designed to minimize the number of security portals and pathways. This can be done with use of service corridors & stairwells that channel personnel from various areas prior to entrance into the SIDA or other security area.

Architectural planning and design can reasonably develop several areas of security within the terminal and develop boundaries between them. The dynamics of airport operation require that all boundaries have strategies for transition across them. The best method is to limit the number of access points to the operationally necessary minimum. If possible, collect 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 interlocked with the security system so that security clearance is required to open the door and closure or alarm is automatic after a programmed delay.

g. Space for Expanded, Additional and Contingency Security Measures

Architectural planning and design typically establishes 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 for expansion and contingencies both reduces cost for the installation and execution of those measures and minimizes the operational impact when those measures are added.

Heightened security levels may require the addition of temporary or relocated checkpoints to facilitate enhanced security processing. This may involve preparing 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 areas, with a need for additional communications and perhaps heating/cooling. Communications and data systems may require temporary expansion and/or remote inputs. Concession spaces that are 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 areas, local artifact or commercial displays, etc., bearing in mind the need for 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.

Section III-D-1 - Terminal Security Architecture Checklist:

- ☐ **Architecture plays a fundamental role in transitioning from public to secured areas**
- ☐ **Design to be flexible; technology, regulations, and threat continues to change**
- ☐ **Carefully coordinate locations for access points and equipment rooms to minimize crossing security boundaries during day-to-day operations**
- ☐ **Planning and Design Considerations**
  - Physical Boundaries
  - Between different regulatory and physical security levels
  - Prevent items from being passed through/over
  - Deter public access to nonpublic areas
  - Provide visual or psychological deterrent
- ☐ **Bomb/Blast Analysis**
  - Critical part of early design considerations
  - Review bomb/blast analysis periodically
- ☐ **Limited Concealment Areas/Structures**
  - Minimize areas where objects or persons can be concealed
  - Minimize and lock accessible spaces and rooms
  - Coordinate with local security, search and threat response agencies
- ☐ **Operational Pathways for:**
  - Passengers
  - Airport Personnel
  - Tenants / Concessions
  - Emergency Response Routes
  - Delivery Routes
  - Security Response
  - Police Escorts for Holding Purposes
- ☐ **Minimum Number of Security Portals**
  - Minimize numbers for cost and security
  - Reduces cost if personnel screening becomes necessary
  - Maximizes use/efficiency of systems
  - Remain flexible for future expansion
- ☐ **Space for Additional Security Measures**
  - Allows growth with minimal impact on operations
  - Reduces installation and execution costs
  - Reduces time needed for additions/expansions
- ☐ **Consider allotting space/accommodations for:**
  - Temporary SSCP
  - Additional SSCP locations
  - Delivery and personnel screening
  - Expansion to planned SSCP (Refer to the *SSCP Section* on page 88 for further information)

2. Terminal Area Users and Infrastructure

a. Users & Stakeholders

The airport operator and air carriers have the primary responsibility for protecting their passengers and employees, although in many cases they share those responsibilities, such as at the screening checkpoint, which has changed from an airline function to a Federal responsibility under TSA. For some other Federal stakeholders, the names have changed, but the underlying operational responsibilities are essentially the same. For example, "Customs and Border Protection" (CBP) and "Immigration and Customs Enforcement" (ICE) now look very different on the Federal organizational chart, and have many new regulations under which they operate. They perform essentially the same functions as their predecessor agencies, and each still must have its security requirements addressed early in the planning and design process. These functions will be considered throughout this chapter, particularly in *Terminal Security Architecture on page 58*, and *International Aviation Security and Its Implications for U.S. Airports* on page 191.

Other users and stakeholders include virtually everyone who sets foot on the airport, although each will operate differently for various reasons. It is important to note that while the prevailing concept in airport security for several years has 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, 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:

1) The passenger is the primary "user" of any terminal building, and the underlying reason for security measures to be in place.

2) Coupled with passengers are the general public and "meeters and greeters," who tend to populate the non-secure public side of the terminal building or the terminal curbside areas but are nonetheless highly important security concerns, both as persons to be protected and possibly as threats to be protected against.

3) Airport and airline employees must have access to various security-related areas of the terminal building to perform their responsibilities. However, not all of the employees require full access to the entire terminal building and all related facilities.

4) Federal agencies typically have regulatory roles including, but not limited to, passenger and baggage screening, customs and immigration functions, and regulatory inspections. Each will require various levels of access to different secured facilities, and occasionally to all areas.

5) Law Enforcement, usually a function of a local political jurisdiction, typically has airport-wide responsibilities requiring full access to all facilities and areas.

6) Concessions can be on the public, sterile and/or secure side of screening, and may require design accommodations that enable certain users access to limited areas and other users to have free access across security boundaries.

7) Cargo operations are usually remote from the main terminal building areas, and will often have separate security design requirements unique to the operator. However, each cargo operation must remain consistent with the Airport Security Program (ASP) and evolving regulatory requirements that are currently leaning toward a more hardened perimeter compared to past requirements.

8) Tenants may or may not be aviation-related organizations, and may or may not have specialized security design requirements, depending on 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 various items through the

security perimeter to the airport for shipment. Similarly, avionics repair shops located in a remote hangar may require access to aircraft to install and test their work.

9) Fixed Base Operators (FBO) for general aviation (GA) aircraft are most often found well removed from the main terminal complex in larger 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.

10) 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.

11) Emergency Response vehicles and persons might come from dozens of surrounding communities and facilities to perform mutual-aid responsibilities in the event of an emergency. This fact drives design considerations for ease of perimeter access, direct routes and access to affected facilities, and quick access to emergency equipment such as water standpipes, electrical connections, stairwells, HVAC facilities and elevator machine rooms, to name just a few.

b. Personnel Circulation

The security designer faces a challenge in modern terminal buildings to provide ease of personnel circulation. 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 without violating the boundaries of sterile or secured areas, particularly those leading to and from administrative areas, boarding gates and passenger hold-rooms, or at baggage claim locations where carousels and doors may directly connect 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 them completely with non-intersecting paths of travel, or it may require methods of access control or directional channeling. Circulation is a double-edged sword; it must provide an optimal amount of access, while not compromising security.

c. Utility Infrastructure

Security aspects of the planning, design and architectural considerations that support necessary utilities in the terminal are discussed in *Power, Communications & Cabling Infrastructure* on page 180.

d. New Construction vs. Alterations

While there is an important distinction between the two concepts of new construction vs. major (or even minor) renovations to an existing building, there is no significant difference from a security standpoint. 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 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. 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 systems such as access control and/or CCTV, and the projected lifespan and/or future changes associated with the building that is being re-designed.

Indeed, those same factors, and possibly others, may help 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 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. For example, in updating an old 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 provisions. A new facility, however, provides a multitude of options for new vertical or horizontal circulation patterns, new entries and exits, new capacities for various terminal building infrastructure requirements (i.e., power, water, HVAC, etc.)

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 apply to new and renovated/expanded structures. The final decisions and outcome for each project will be very different. This document can help guide the designers through the process.

Section III-D-2 - Terminal Area Users and Infrastructure Checklist:

- ☐ **Meet with all relevant airport users and stakeholders, including tenants and government agencies.**
- ☐ **Personnel circulation includes vertical separation as well as horizontal (elevators, escalators, stairwells)**
- ☐ **Supporting utility infrastructure (power, data, communications) is an equally important element of security design**
- ☐ **New Construction vs. Alterations – both require the same attention to security**

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. The sterile area is controlled by inspecting persons and property in accordance with the TSA-approved airport security program (ASP). The primary objective of a sterile area is to provide a passenger holding and 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:

a. All portals that serve as potential access points to sterile areas (i.e., doors, windows, passageways, etc.) must be addressed to prevent bypassing the security screening checkpoint. The number of access points should be limited to the minimum that is operationally necessary.

b. Portals, including gates and fire egress doors, must restrict unauthorized entry by any person to the sterile are, and to the secured area, which is generally airside. Doors must also comply with local fire and life safety codes, Americans with Disabilities Act (ADA) requirements, and other applicable requirements. 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 the need for and how to accomplish the securing of fire doors.

c. Sterile areas should be designed and constructed to prevent articles from being passed from non-sterile areas to sterile or secured areas. Designs should prevent passage of unauthorized items between non-sterile and sterile area restrooms, airline lounges and kitchen facilities, such as through plumbing chases, air vents, drains, trash chutes, utility tunnels or other channels.

d. When planning the construction of non-sterile or public access suspended walkways or balconies over or adjacent to sterile areas, it is extremely important to consider effective barriers to prevent passing or throwing items into sterile areas.

e. During planning and layout of sterile areas, consideration must be given to the access needs of airport and airline personnel, maintenance and concession staff and supplies. Specific items for consideration include:

   1) Tenant personnel and airport employees who require access into the sterile area from public occupancy areas;

2) Emergency response routes and pathways should be nonpublic, easily accessible, never blocked by boxes, bins, or other hazards, and provide clear, quick access for any emergency equipment needed (i.e., stretchers, wheel chairs, explosives detection/ transportation equipment, paramedic equipment, etc.). Routes for off-airport response (emergency medical services [EMS] and fire personnel) should also be considered.

3) Concessionaire deliveries and supplies should be considered as a part of the planning and design process. Concessionaires are typically located within the sterile areas. Concessionaires and other airport tenants typically receive deliveries at all times of the day. These deliveries are 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. The planning process should develop strategies for concessionaire deliveries, storage areas, employee access routes, and space flow. These require adequate attention to security levels to prevent obstructions and patron queuing areas near or in security checkpoint areas, and to eliminate the occurrence of non-identified/non-credentialed and unscreened delivery and concessions personnel within the sterile area. All such screening should take place well away from designated passenger screening areas.

f. 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 person who has been screened and is in the sterile area.

g. Security of sterile areas is improved with design solutions that are oriented toward deterring the concealment of deadly or dangerous devices. Built-in fixtures (i.e., railings, pillars, benches, ashtrays, trash cans, etc.) designed to deter and/or hinder the concealment of weapons or dangerous devices are widely available.

Section III-D-3 - Sterile Areas Checklist:

☐ **Sterile Areas**
- Refers to the area between the security screening checkpoint and the loading bridge and/or hold room door.
- Primary objective; passenger containment, preventing access to weapons or contraband
- Number of access limited to the minimum operational necessity
- Comply with local fire and life safety codes, Americans with Disabilities Act (ADA), etc.
  - Prevent articles from being passed from non-sterile areas to sterile or secured areas
  - Consider pathways in restrooms, airline lounges, kitchen facilities, plumbing chases, air vents, drains, trash chutes, utility tunnels or other channels
  - Consider access needs of airport and airline personnel, maintenance and concession staff and supplies
- Tenant personnel and airport employees who require access into the sterile area from public occupancy areas
- Emergency response routes and pathways
- Routes for off-airport response, emergency medical services [EMS] and fire personnel
- Concessionaires have unique access, delivery and storage requirements beyond security, including perishables
- Built-in security-friendly fixtures (i.e., railings, pillars, benches, ashtrays, trash cans, etc.) are widely available

4. Public Areas

One of the most challenging issues faced by the planning and design team is not only to make the best possible operational, economic and business use of space within the terminal, but in doing so, to provide the passenger and public an acceptable level of comfort for their experience. 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, and whether they will be comfortable.

IATA's Airport Terminal Reference Planning Manual defines levels of service as indicated in *Table III-D-1* below, with Level C or higher being the typical goal:

Table III-D-1 - Levels of Service Definitions

LOS	Definition
A	Excellent LOS, condition of free flow, no delays, excellent level of comfort
B	High LOS, condition of stable flow, very few delays, good level of comfort
> C	Good LOS, condition of stable flow, acceptable delays, good level of comfort
D	Adequate LOS; condition of unstable flow, acceptable delays for short periods of time; adequate level of comfort
E	Inadequate LOS; condition of cross-flows, system breakdown and unacceptable delays, inadequate level of comfort
F	Unacceptable LOS; condition of cross-flows, system breakdown and unacceptable delays; Unacceptable level of comfort

However, there are both qualitative and quantitative components to LOS considerations – whether they will be comfortable, whether it is convenient and efficient, and whether the throughput is sufficient to accomplish the goal. J.J. Fruin's work, in Pedestrian Planning and Design, was originally based on bus terminals, and looked simply at the spaces surrounding passengers carrying baggage, while IATA distinguishes between types of queue – (i.e., passengers with/without bags). Refer to *Table III-D-2* and *Table III-D-3* below for further information.

Table III-D-2 - Fruin's Queue Level of Service C = 7-10 SF per person

	Description	SF per person
A	Free circulation zone	13 or more
B	Restricted circulation zone	10-13
> C	Personal comfort zone	7-10
D	No-touch zone	3-7
E	Touch zone	2-3
F	Body ellipse	2 or less

Table III-D-3 - IATA Level of Service C = 11-17 SF per person

Terminal Area	LOS	Check in Queue	Wait/Circulate	Hold Room	Bag Claim	FIS
Allocated Square Feet per Person	A	19	29	15	22	15
	B	17	25	13	19	13
	> C	15	20	11	17	11
	D	13	16	9	15	9
	E	11	11	6	13	6
	F	System Breakdown				

Figure III-D-1 below illustrates the relative space available under Fruin's concepts; IATA figures would provide somewhat more space per person. It is difficult to make an objective level of service determination because, by definition, LOS is subjective. In addition, there is another dimension to that subjectivity, one of time – whether the space allowed by your calculations allows the necessary movement and speed of throughput to accomplish the goals set for queuing time and reduced congestion at the ticket counter, in the corridors and concourses, at the screening checkpoint, on elevators and escalators, and anywhere else people are moving through the terminal buildings.

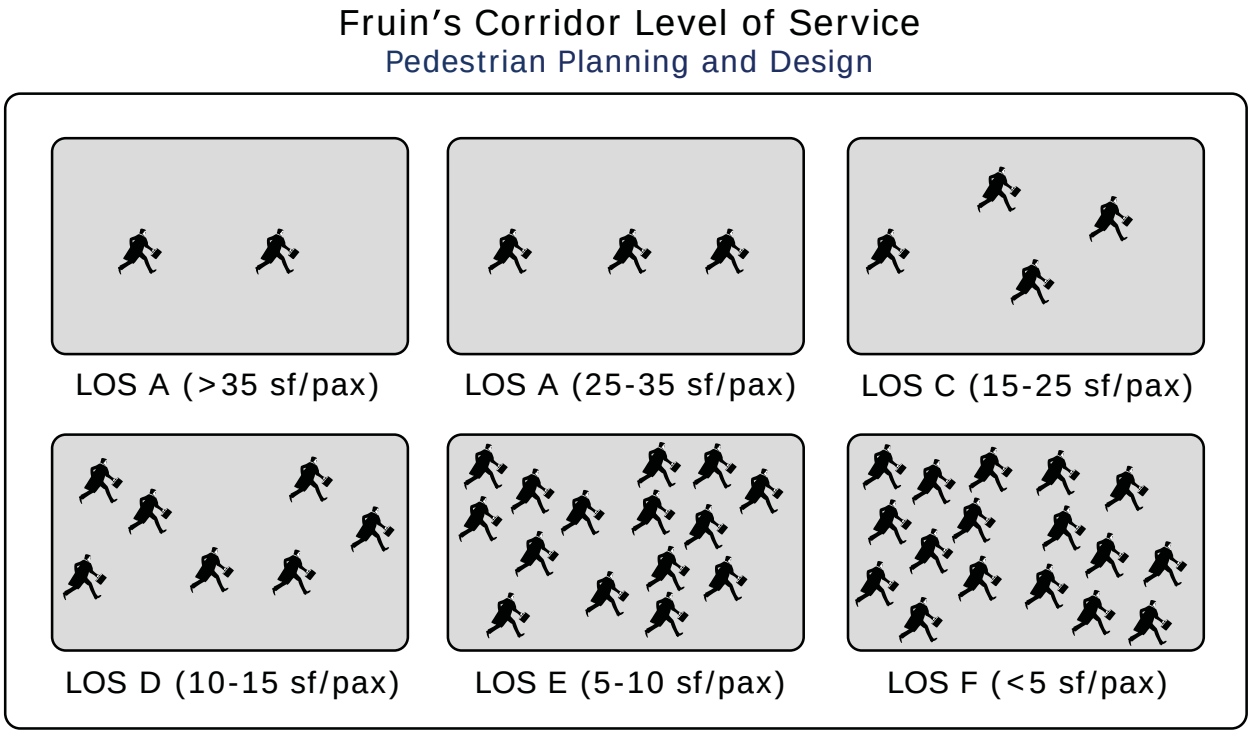


Figure III-D-1 - Visual Depiction of Density in Levels of Service

Simulation modeling can assist the designer in determining the optimum balance of space, which may very well be quite different from one area to an adjacent one in both public and non-public areas. Various other means of determining LOS estimations can be found in Chapter 5 of A/C 5360-13, and in *Appendix B* of this book.

a. Public Lobby Areas (Ticketing, Bag Check and Claim, Rental Car)

Security can be greatly improved by limiting the number of access points, and by CCTV-monitoring all access points (to include conveyor belts) through which direct or indirect access from public areas to the airside can be gained.

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 pose an attractive target. Promoting the free flow of passengers requires adequate capacities at every stage, including curbside check-in, ticket counters, SSCPs and vertical transportation to meet peak hour flows. It is also 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 with the time passengers spend going thru passenger screening to avoid excessive queuing at either location.

2) Configuration of Domestic Baggage Claim Areas

The current designs of the claim areas for baggage arriving on domestic flights include vulnerabilities that should be hardened in new designs. Such features as claim areas accessible from the street, bags stored on floors, 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' secure 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, 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 incorporate federal inspection services' functions, which domestic arrival areas need not do.) It is recognized that it is not practical to re-construct 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, the secure (international) layout of baggage claim areas can easily 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 bag claim areas, so that there are no exit lanes adjacent to the screening checkpoint, thus eliminating a common security concern of checkpoint breaches.

Consider ways of both visually and physically differentiating between public and sterile or non-public areas in terminal design to deter and prevent entry by unauthorized persons. Segregation of these areas requires a capability to secure or close down areas not in use.

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 improvised explosive device (IED). 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 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 blast analysis plan (BAP) and vulnerability assessment in accordance with DHS/TSA guidelines may be desirable.

Advances in technology will result in new ways of doing business. Some airline passengers may check in at a remote location, such as a downtown hotel ticket office, or a cruise ship terminal. Many airlines 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 must 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 is one of "chain of control" 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. This concept is addressed in further detail in *Remote Baggage Check-In* on page 144.

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 who may need to apply additional security measures during the passenger check-in process. In some cases, additional space is required to support aircraft operator interviews of passengers and x-ray or search of baggage prior to issuance of boarding gate passes. Additional queuing space may also be required.

b. 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 unsecured or inadequately secured access to secured areas.

Consider equipping emergency exit doors with local and/or monitored alarms that can be heard and responded to quickly by staff. The need and location of such emergency exits must be coordinated closely with the local Fire Marshall and/or code officials. Whenever possible the terminal building should be designed such that emergency exits leading into secured areas are minimized and such that 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 re-screen 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 must be paid to the potential for mass evacuation, whether during an actual emergency or when a concourse may have to be cleared when a breach has occurred. In either such case, the designer must 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 re-screening 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, use of monitoring systems such as CCTV, and use of monitored door alarms can drastically reduce incidence of false alarms and the need for officer dispatches and other responses to security breaches.

c. Security Doors vs. Fire Doors

Security and safety are sometimes at odds, as airport experience 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.

It should be noted that a key component of the physical security system within the federal inspection services (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 be secure and sterile to prevent smuggling aliens, terrorists, criminals and contraband into the United States. Guidance on FIS design requirements is found in *the International Section* on page 191.

The planner and designer should keep the number of AOA access points to an operational minimum, and wherever possible have fire doors open into non-secured areas so that a delayed release is not required. However, reverse use of such exits – proceeding against the flow to enter the sterile area from the non-secured area – must also be considered, and surveillance systems or other means employed to detect, deter or prevent a breach of security.

d. Concessions Areas

Concessionaires are a major source of airport revenue and are typically located throughout an airport terminal facility on both sides of security. It is usually economically advantageous to the airport to make

concessions areas accessible to the broadest possible range of visitors and passengers. Post-9/11 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.

In designs where the majority of concessions are within the sterile area, it can be advantageous to design the concession layout in such a way that temporary, alternate locations for the screening checkpoints can be used during heightened security periods, to remove concessions from the sterile area.

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

Concessions at an airport vary in function and operation. 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 deliveries from various suppliers and various types and locations of 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, storage access), and its individual security requirements (duress alarms, CCTV, ATM security, armed guard escorts).

Due to the variety of concession types and operations, concessionaires or designated representatives should be involved in the design and coordination process with the airport owner and airport security personnel. Since concession companies and types change, 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 identification 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 U.S. Mail), design considerations (access point locations and types, loading dock, phone, locations of concessions storage and mail areas) that complement these procedural issues can minimize the security risks with proper coordination. A key security risk when deliveries are escorted into the sterile or other security areas is that 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 manned visitor/escort sign-in/out station which requires both the escort and escortee to be present both entering and exiting. If the accommodation for such a station is not or considered in the design phase, it may be difficult to execute later on.

To summarize, concession design considerations include: locating concession storage areas in public or non-secured/low-risk areas, design/use of a separate loading dock/concessions screening area for personnel and/or packages, location of concessions and/or public mail areas outside of security areas, simplification and shortness of the delivery access routes and the quantity of security access points which must be used (an "escort-friendly" design), visitor/escort sign-in/out stations, and careful planning of which concessions should be within security areas based on their delivery and personnel requirements.

e. Signage

Having clear, easily understood signage is important for accommodating the control and expeditious flow of passengers, meeters-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 (FIDS) and multi-user flight information displays (MUFIDS, regulatory signs, and construction and advertising signs.

In addition to airport preferences, signage must take into account security requirements of the FAA and TSA, certain standards of the U.S. Department of Transportation and State transportation departments, and requirements of the Americans for Disabilities Act (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 problem areas, message conflicts, and common nomenclature provide the designer with a basis for programming the signs. These elements are important to security because they convey information needed to understand the process required and/or personal options 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, infrequent users and the disabled community.

Signage can be classified as (a) static, such as directional symbols and room labels, and (b) dynamic, which includes constantly updated directories and 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 security events and emergency situations when warnings and instructions for passengers and support personnel can prove most valuable. To be effective, these capabilities must be identified early in the planning and design process to assure 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 the operational authority, to control what, where, and how information is routed to interior and exterior signage during such conditions.

There is currently 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 multi-lingual global marketplace, 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.

1) List of authorities affecting interests in signage at airports:
    a) Accessibility
        i) Americans with Disabilities Act (ADA)
        ii) Americans with Disabilities Act Accessibilities Guidelines (ADAAG)
        iii) Disability and Senior Citizen Groups
        iv) State Accessibility Codes
    b) Government Agencies
        i) Federal Aviation Administration (FAA)
        ii) Department of Transportation (DOT)
        iii) Department of Justice (DOJ)
        iv) Occupational Safety & Health Administration (OSHA) Port Authority
    c) Federal Inspection Services
        i) Customs and Border Protection (CBP)
        ii) Animal and Plant Health Inspection Service (APHIS)
        iii) Fish and Wildlife Service (FWS)

iv) Center for Disease Control (CDC)
v) Public Health Service (PHS)

d) Building Code Compliance
i) Local building and fire codes
ii) State building and fire codes
iii) Electrical Code
iv) Life Safety

e) Security
i) Airport Police
ii) Transportation Security Administration (TSA)
iii) Department of Homeland Security (DHS)
iv) Foreign Language Specialists (Translation Services)
v) Media Relations/Public Relations

2) Signage specific coordination required:
a) Electrical (providing power and data to signs)
b) Video/Cameras (obstructions)
c) Sprinkler Systems (obstructions)
d) Lighting (obstructions and/or external illumination of signs)

f. Public Lockers

Public lockers have been used to conceal explosive devices in airports and other transportation terminals around the world. From a security viewpoint, the appropriate location for unmonitored public lockers is within sterile areas beyond the security screening stations. If placement in sterile areas is not possible, consider eliminating lockers or subjecting them to constant surveillance, as well as structural enhancements to the surrounding area.

Any such lockers, left-luggage or storage areas should be designed so as to accommodate an appropriate level of screening required by TSA of any packages or luggage that is checked by passengers or is to remain otherwise unattended.

g. Unclaimed Luggage

Consideration must 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 must be considered

h. VIP Lounges/Hospitality Suites

Some airports feature VIP lounges and/or airline hospitality suites, which are frequently 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.

i. Vertical Access

Prevent the traveling public from accessing the airside though connecting elevators, escalators and stairwells.

j. 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.

Section III-D-4 - Public Areas Checklist

- ☐ Public Areas
  - Public Lobby Areas (Ticketing, Bag Claim, Rental Car)
    - Limit the number of access points
    - Monitor all access points and conveyor belts via CCTV
    - Visually differentiate public and secure or restricted areas
    - Build in a capability to secure areas when not in use
    - Select furnishings and accessories which avoid the concealment of explosives
    - Seek advice from structural and explosives experts on minimizing the effects of blast
    - Ticketing Lobby
      - Minimal seating in ticketing lobbies will reduce congestion
      - Consider the needs of international or high-risk aircraft operators with extended security measures during the passenger check-in process
      - Additional queuing space may be required
  - Public Emergency Exits
    - Some exit requirements have specific widths and separation distances
    - Coordinate locations closely with the Fire Marshall and/or Code officials
    - Emergency exits should avoid moving persons from areas of lower security to areas of higher security
    - The number of emergency exits leading into secured areas should be minimized
    - Exiting screened individuals should be kept separate from unscreened individuals
    - Consider emergency doors with push-type panic bars with 15-30 second delays (where allowable)
    - Security Doors vs. Fire Doors
      - If the door is not a fire door, make it lockable
      - Emergency egress door (fire door) may not be locked
  - Concessions Areas
    - Consider a design to accommodate moving concessions (or screening points) during heightened security
    - Some concessions require storage and processing space
    - Look for short delivery and personnel access routes that minimize crossing security boundaries
    - Consider type of concession, delivery, storage, moneyhandling and security escorts, ATM security
    - Design elements for concessions include:
      - Locate concessions storage areas in public or nonsecured /low-risk areas
      - Separate loading dock/concessions screening area from passengers and secured areas
  - Vertical Access: Prevent public access to the airside though connecting elevators, escalators and stairwells
  - Signage: Types of agencies with interests in signage at airports:
    - Accessibility
      - Americans with Disabilities Act (ADA)
      - Americans with Disabilities Act Accessibilities Guidelines (ADAAG)
      - Disability and Senior Citizen Groups
      - State Accessibility Codes
    - Government Agencies
      - Federal Aviation Administration (FAA)
      - Department of Transportation (DOT)
      - Department of Justice (DOJ)
      - Occupational Safety & Health Administration (OSHA) Port Authority
    - Federal Inspection Services
      - Customs and Border Protection (CBP)
      - Animal and Plant Health Inspection Service (APHIS)
      - Fish and Wildlife Service (FWS)

    - Center for Disease Control (CDC)
    - Public Health Service (PHS)
  - Building Code Compliance
    - Local building and fire codes
    - State building and fire codes
    - Electrical Code
    - Life Safety
  - Security
    - Airport Police
    - Transportation Security Administration (TSA)
    - Department of Homeland Security (DHS)
    - Foreign Language Specialists (Translation Services)
    - Media Relations/Public Relations
  - Signage specific coordination required:
    - Electrical (providing power and data to signs)
    - Video/Cameras (obstructions)
    - Sprinkler Systems (obstructions)
    - Lighting (obstructions and/or external illumination of signs)
- Lockers:
  - Eliminate public lockers from public areas where possible
- Unclaimed luggage areas – landside, with easy EOD / LEO access
- VIP Lounges/Hospitality Suites
  - Consider location in relationship to sterile area
  - Prevent unauthorized access to secured and sterile areas
  - Provide space for monitored baggage holding facilities
- Observations decks are strongly discouraged - Where they exist, they should be closed to public access

5. Nonpublic Areas

a. Service Corridors, Stairwells and Vertical Circulation

1) Public areas, secure 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 and controlled. (Service corridors may be desirable to enhance 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.)

2) Service corridors may also be used to minimize quantity and type of security access points. If access requirements are clustered or grouped 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 security than one access point per use or user.

3) The planning and design of non-public service corridors should consider their placement and possible use by airport emergency personnel and law enforcement officers (LEOs). While use of service corridors by emergency and LEO agencies 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.

4) Vertical circulation and stairwells are more difficult to control than corridors. They typically 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.

5) When coordinating stairwells and vertical pathways, care must be given to security treatments and boundaries. Since many of these vertical pathways function not only as emergency pathways, but also as service pathways, the quantity and type of security treatments should be carefully considered. In addition, as with any fire exit, permissible door equipment and delays must be carefully coordinated with the local code and building officials.

b. 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 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. Thus 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, as necessary, 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 their need for visitors and public access, as well as the likelihood that those visitors might be inadvertently left unattended or unescorted, having unintended access to security area.

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 a concern. When airport authority/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 potential design considerations include: security of airport personnel and financial records, security of access control and ID workstations, security of identification media stock and records, safe and money storage areas, and computer server and equipment areas, especially for security-related facilities such as the access control system.

c. Tenant Spaces

There is no fixed rule on whether tenant spaces require tie-in to the access control system. Indeed, there are no such regulatory requirements for tenant security, although if the airport wishes to include tenant areas, it is wise to design a single unitary system rather than try to integrate multiple tenants 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, overnight cargo and maintenance operations, late night or early morning concession deliveries, etc.

d. Law Enforcement & Public Safety Areas

Guidance materials encourage the provision of supporting facilities for security services at airports serving civil aviation. ICAO Annex 17 contains *"Standards and Recommended Practices"* (SARPs), and although the United States is a signatory to ICAO, these are minimum recommendations not specifically required by TSA regulations, which in most cases are generally more exacting.

1) Public Safety or Police Offices

   a) Office space for airport security or law enforcement personnel should be provided in or near the terminal building, and be sized after thorough discussions with police officials and the airport operator.

   b) Police facilities in the terminal complex should be planned to allow public access to a controlled meeting area to mitigate the effect of a detonated device and/or small arms fire. This might include ballistic materials, window laminates, and concrete bollards/planters to prevent vehicular penetration.

   c) Satellite police facilities can be distributed throughout the terminal to improve response times to widely separated facilities, as well as reduce vulnerability to a single point of attack.

   d) Physical infrastructure might consider adequate space for:

      i) Briefing/work room
      ii) Training classroom/offices
      iii) Property/evidence room(s)
      iv) Conference rooms—can be part of CP/operations room(s)
      v) Holding cells
      vi) Satellite locations, if used
      vii) Private Interrogation/Witness Statement room(s)/area
      viii) Lockers, showers, and restrooms
      ix) General storage areas
      x) Secured arms storage
      xi) Kitchen/lunchroom facilities

   e) Areas requiring access for public and tenants, protected with adequate controls, include:

      i) Administrative offices
      ii) Security ID offices (if handled by LEOs)
      iii) Lost and found
      iv) Training rooms
      v) Medical services

   f) Consideration must be given to electrical, fiber optic and other utility supply and routes to/from the police areas. In addition to special consideration of need for such additional secure communications technology as NCIC, FBI, Federal task forces and other liaison, attention must also be given to the amounts of conduit required to accommodate future expansion in this era of rapidly increasing security requirements and government liaison.

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, with quick access capability in both directions integrated with the access control system. Consideration should also be given for helicopter pads (when applicable) to be located in secure areas, including rooftops if appropriate.

3) Remote Law Enforcement/Public Safety Posts/Areas

   a) In large facilities, remote areas, or where minimized response time is a concern, 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.

   b) 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.

   c) 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.

4) Other Considerations

a) Communication/Dispatch facilities, equipment repair areas and other support functions near the police functions should be located away from high threat areas and be considered for protection and control treatments.

b) Many airports, because of size, activities, budget(s), and political or joint working arrangements with local police organizations, may combine or contract out some security activities. This does not lessen 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 space.

c) Some airports prefer to maintain control of their 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 who has 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.

d) Some airports prefer to maintain control of their 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 who has 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.

e. Explosives Detection Canine (K-9) Teams and Facilities

1) 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, 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 diverted for temporary “visiting” K-9 use.

2) There are no specific technical requirements, 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.

3) The investment in dogs and their training is large; 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.

4) 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 areas of the airport as parking lots, cargo ramps, baggage make-up and bag claim areas, to maintain a realistic training environment.

5) The designer must consider providing as much isolation as possible from airport noise and odor sources, especially jet fuel fumes, since the dog’s sense of smell is critical to its mission. The administrative area should also have secured storage for live or dummy explosives test and training items; these areas should be coordinated with ATF regulatory requirements for storage of explosives. Also consider reasonable proximity to EOD personnel and to threat containment units, as well as adequate parking nearby for K-9 transport vehicles.

f. Security Operations Center (SOC)

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, including: Airport Communications Center, Airport Operations Center, or Security Control Center.

An SOC can provide multiple communications links to the airport operator including police, fire, rescue, airport operations, crash/hijack alert, off-airport emergency assistance 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 to the console facilitates equipment installation, maintenance and upgrades.

Connecting all airport security sensors to the SOC facilitates verification of the operability of each of the sensors. Sensors can periodically be commanded to go into alarm states, with the response checked by the SOC. 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 Command Post, and in a secure area. From the standpoint of cabling interconnections, a relatively central geographic location serves to maintain reasonable cable lengths to all 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 and operate in a cost-effective manner.

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

a) Access terminals for law enforcement informational systems such as CAD, NCIC, etc.
b) Automatic Notification System for emergency response recall of personnel
c) Direct phone lines to ATCT tower, airlines, airport mini hospital, etc.
d) Airport Emergency Command Post
e) Fire Alarm monitoring
f) Flight Information Display (FIDS) systems; Baggage Information Display (BIDS) systems
g) ID Department
h) Information Specialists for customer information lines, courtesy phones, airport paging
i) Landside/Terminal Operations
j) Maintenance Control/Dispatch or Alarm Monitoring (includes energy management of HVAC systems)
k) Monitoring of public safety, duress or tenant security alarms
l) Personnel Paging System
m) Police and/or Security Department
n) Radio Systems
o) Recording Equipment
p) Weather Monitoring/Radar/Alert systems

In sizing the SOC and determining its equipment requirements, it is useful to consider, especially for Cat X and other higher-risk airports, whether there is enough physical room, electronic accommodation and operational capacity beyond a "normal" emergency load, to handle multiple simultaneous events. For example, this might include a requirement to provide separate video and communications channels to two highly diverse locations for very different events.

g. Airport Emergency Command Post (CP)

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 conference or meeting rooms.

1) Location

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

   b) 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.

   c) 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 sound proof.

   d) A Mobile CP is a viable option at many airports, but requires allotments of support space and a coordinated communications infrastructure.

2) 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. Designer and planner are referred to the requirements of the Airport Emergency Plan and the Airport Security Program to determine the optimum number of persons to be accommodated; information found in Advisory Circular 150/5200-31A, Airport Emergency Plan, can assist.

3) Other Considerations

   a) 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.

   b) CP electrical power must be uninterrupted, which is accomplished by a dedicated uninterrupted power supply within the CP itself or by being linked to a "no-break" power source or generator.

   c) Secure vehicular access to the CP should be considered.

   d) Sufficient controlled vehicular parking areas on either the landside or the airside and in close proximity should be provided for support vehicles (fire, catering, off-airport mobile communications vehicles, etc.) and key CP vehicles.

   e) Consider the placement of an Executive Conference Room adjacent to the CP for executive briefings and conferences.

   f) Provide space for kitchenette and rest rooms, and rest/sleep facilities for long term events.

h. Family Assistance Center

Consideration should be given to dedicated or easily converted space for use as a Family Assistance Center (FAC). The FAC should be easily controlled from an access standpoint, have required 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 at *www.ntsb.gov*.

i. Federal Inspection Service (FIS) Areas

The Federal Inspection Service (FIS) area (if one is to be part of the airport) 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 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 the *International Security* section on page 191. In addition, there is extensive material provided by Customs and Border Protection (CBP), which publishes a separate document that more fully specifies additional security design requirements for FIS space. Consult with local CBP and other FIS representatives to assure use of the most current version of standards, and to coordinate requirements with the CBP and other FIS agencies early in the design process. FAA Advisory Circular 150/5360-13, Planning and Design Guidelines for Airport Terminal Facilities, also provides information relating to the FIS agencies.

j. Loading Dock & 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 daily. People who use the airport loading docks and delivery areas should be appropriately equipped with identification media and subject to vehicle inspection. Consideration should be given to using a remote, consolidated distribution center (separated from the terminal or at the far edge of the terminal) that provides the airport an opportunity to screen deliveries prior to entry to the airport. Some airports have chosen to implement night deliveries to lighten truck and van traffic around the airport during the day. Of necessity, 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 delivery recipients, various methods of transport and security control may 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 identification media, screening of delivered merchandise, and CCTV monitoring are all potential methods of control.

Space should be allocated and configured for physical inspection of vehicles and their contents. During heightened security conditions, physical inspection of all delivery vehicles approaching the terminal might be required. As such, considerations for at least temporary vehicle inspection points should be made.

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 bombs. 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.

Section III-D-5 - Nonpublic Areas Checklist:

☐ **Non-Public Areas**

- Service Corridors, Stairwells and Vertical Circulation
  - Service corridors should not cross boundaries of secure areas
  - Service corridors may be used to minimize quantity of security access points
  - Tenant areas can be grouped into common service corridor
  - Consider corridor placement and use by airport emergency personnel and law enforcement
  - Fire stairs typically connect many of the building's floors/levels as well as security areas
  - Stairwells and vertical pathways may require security treatments and boundaries
- Airport Personnel Offices
  - Office areas should connect via corridors and stairs to minimize the need to cross security boundaries
  - Office spaces should be planned to accommodate visitors and public access
  - Consider the use of satellite police, ID or first aid offices
- Tenant Spaces
  - Some tenant spaces might require tie-in to the airport access control and alarm system
  - Consider tenant money-handling, overnight operations, early morning concession deliveries
- Law Enforcement & Public Safety Areas
  - Public Safety or Police Offices
    - Office space for airport law enforcement in the terminal
    - Public access area protected with ballistic materials, laminates, concrete bollards, etc.
    - Include adequate space (in no particular order) for:
      - Briefing/work room
      - Training classroom/offices
      - Property/evidence room(s)
      - Conference rooms—can be part of CP/operations room(s)
      - Holding cells
      - Possible satellite locations
      - Private Interrogation/Witness Statement room(s)/area
      - Physical fitness area in conjunction with lockers, showers, and restrooms
      - General storage areas
      - Secured arms storage
      - Kitchen/lunchroom facilities
    - Areas requiring access for public and tenants but protected with adequate controls are:
      - Administrative offices
      - Security ID offices
      - Lost and found
      - SIDA/tenant training rooms
      - Medical services
    - Consider electrical, fiber optic and other utility supply and routes to/from the police areas
  - Law Enforcement Parking
    - Accessible, with direct landside/SIDA access
  - Remote Law Enforcement/Public Safety Posts/Areas
    - Consider remote law enforcement posts or substations; outdoor shelters
  - Other Considerations
    - Communication/Dispatch facilities
    - Equipment repair areas
- Dogs/K-9 Teams
  - If there is no on-site K-9, specify non-critical area for temporary K-9 use
  - Rule of thumb: a 4- by - 8-foot indoor pen, 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, dry environment, without mildew or dampness
- The dog area should be secured, and sufficiently isolated from casual public contact
- Provide areas for veterinarian services and training activities
- Isolation from noise and odor sources, especially jet fuel fumes
- Secured storage for explosives test and training items; coordinated with ATF
- Consider proximity to EOD personnel and to threat containment units

- Security Operations Center (SOC)
  - Consider multiple communications options for police, fire, rescue, airport operations, crash/hijack alert, off-airport emergency assistance, and security of communications
  - Locate close to the Airport Emergency Command Post (CP), in a secure area
  - For cabling interconnections, a central geographic location maintains reasonable cable lengths
  - Floor space, cabinets, power, HVAC, fiber optics and cabling, and conduit paths
  - Rear access to console for maintenance and update.
  - Consider space requirements of consolidating all functions within the SOC:
    - Airport Police and/or Security Department
    - Automatic Notification System for emergency response recall of personnel
    - Direct phone lines to ATC tower, airlines, airport mini hospital, etc.
    - Fire Alarm monitoring
    - Flight Information Display (FIDS) systems; Baggage Information (BIDS) systems
    - ID offices
    - Information Specialists for customer information phones, paging;
    - Landside/Terminal Operations
    - Maintenance Control/Dispatch (includes total energy management of HVAC systems)
    - Airport Radio and Personnel Paging Systems
    - Recording Equipment
  - Plan an alternate site capable of supporting the basic operation.
  - A direct view of the airside and the isolated parking position is desirable.
  - Space Needs
    - Space for Crisis Management Team's Operational Group and Negotiators
    - Advisory Circular 150/5200-31A on airport emergency planning can assist
  - Other Considerations
    - Raised flooring is an option for installation of ducts and cable paths.
    - CP electrical power must be uninterrupted
    - Vehicular access to the CP necessary
    - Controlled parking for support vehicles and key CP vehicles
    - Provide space for kitchenette and rest rooms.
- Family Assistance Center – designated space in the case of an accident or incident.
  - FIS areas are designed toward very different law enforcement and security situations
  - FIS agencies publish a separate document that provides their additional security design guidelines required within their operational spaces
  - Reference FAA Advisory Circular AC 150/5360-13
- Loading Dock & Delivery Areas
  - Access control and identification media
  - Package screening
  - CCTV
- FIS Areas

SEE: FAA Advisory Circular 150/5360-13, Planning and Design Guidelines for Airport Terminal Facilities.

6. Common Use Areas

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

Airports now offer Common Use Passenger Processing Systems (CUPPS). 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 using a reduced number of ticket counter positions and gates; effectively CUPPS will reduce the need the need for territorial expansion or defer expansion to a later date. Inherent in a CUPPS is the airport's ownership of computers, cabling, loading bridges, bag belts and the maintenance thereof. Airports are also branching out by becoming the single-source entity to provide above and below using services to include fueling airline aircraft. This results in a consolidation of personnel and equipment necessary to handle airline aircraft.

7. Terminal Vulnerable Areas & Protection

Terminals are not isolated entities but are part of complex, integrated developments that provide the basic and varied services of a modern airport. This integration of the terminal with other areas suggests 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. Planning and design must 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 must 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. Consider controls on such access points. .

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 must 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 must to 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 vulnerability. The planning and design of these systems must consider not only terminal security, but where the conveyances cross through or above portions of the airside.

Section III-D-6 - Terminal Vulnerable Areas and Protection Checklist:

- ☐ **Due to the complex/multi-use function of terminals they contain the broadest range of vulnerable areas**
- ☐ **Each airport is unique and must 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 adjacent 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 and switching gear
  - 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

8. Chemical and Biological Threats

Airport planners must also be cognizant of the chemical and biological threats to their facilities. Although it is not outside the realm of possibility that a chem/bio attack could be launched against any element of an airport to disrupt the overall operation, the passenger terminal is seen as the most likely target. Preparation for the building of a new terminal or airport facility should be planned to accomplish two objectives:

(1) To deter high-consequence attacks through HVAC system physical security, and;
(2) 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 chemical and biological terrorism would involve substantial effort and cost. The first step is to identify those groups that should be involved in 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, and;
- What are plausible release devices and plausible 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 or HVAC characteristics, 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, depending on the extent desired; 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; and
- Attack mitigation through active response, i.e., actions to take in the event that a suspected attack is discovered. These might include quarantine facilities, detoxification facilities, medical mutual aid response capabilities, and screening of vehicles, among others.

One consideration for implementation is the use of chemical and biological detection systems for building protection. As of publication, there are two types of systems currently in operational use. Chemical sensors that can detect some classes of agents are deployed operationally to provide early warning of chemical releases and to enable rapid and effective facility responses. For example, such a system has been in operation in the Washington D.C. Metro for several years. As of publication, real-time biodetection equipment is not sufficiently mature for operational systems. However, the Department of Homeland Security 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 rapid responses, but does allow exposed individuals to be identified and treated before they become ill, significantly improving their chances of survival, and also allows contaminated facilities to be identified and isolated, preventing additional exposures and additional spreading of contamination. Airports should research the potential and operational uses of detection technologies available at the time.

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"* (SAND2005-0145 and/or LBNL-54973/Rev 2.1), developed by Sandia National Laboratories and Lawrence Berkeley National Laboratory under the Department of Homeland Security'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 (chem-bio) attack, given the technologies and capabilities available today. With the report, airport planners should gain an understanding of the important issues for chem-bio defense, and should be able to assess the preparedness of their airport, to determine whether to bring in consultant expertise, and to target the most effective upgrades for their facilities.

The report has been distributed electronically by the Transportation Security Administration (TSA) to the TSA Federal Security Directors at the top threat airports, and by the Airports Council International and the American Association of Airport Executives to airport executives and security planners. If unable to obtain the report through these sources, a copy may be obtained through Sandia National Laboratories or Lawrence Berkeley Laboratory directly. An excerpt of the report is available in Appendix G.

Section III-D-7 - Chemical & Biological Agent Checklist:

- ☐ **Sources of guidance may include TSA, Federal Emergency Management Agency (FEMA), Federal Bureau of Investigation (FBI), Department of Energy (DOE), Center for Disease Control (CDC), and Office for Domestic Preparedness Support.**
- ☐ **Consider HVAC characteristics such as position of vent intakes and whether HVAC supply for emergency operations center can be targeted from public spaces.**
- ☐ **Consider HVAC system capacity for airflow management.**
- ☐ **Consider areas for quarantine, detox, chem-bio screening of people and vehicles; capacity to accommodate outside mutual medical aid**
- ☐ ***See also*, Edwards, Dr. Donna M., *et al,* "Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism," Sandia Report SAND2005-3237, Berkeley Lab Report LBNL-54973 (May 2005), Prepared by Sandia National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550.**

Section E - Security Screening: Passenger Checkpoints, Baggage and Cargo

This section addresses the unique characteristics of the three very different aspects of TSA–mandated screening:

- The *Security Screening Checkpoint (SSCP)* section on page 88 deals with the area where the traveling public is subjected to the screening of their persons and property when passing from the public areas prior to entering the sterile area of the airport to wait for departure of their flight. It will examine the space, layout and infrastructure requirements solely of that area most familiar to the public.
- The *Baggage Screening* section on page 115 will deal with those areas where checked baggage is screened for explosives and other anomalies prior to loading on an aircraft. There are numerous alternatives to be considered, depending on types of equipment, space constraints and limitations, infrastructure requirements, and operational trade-offs.
- The *Cargo Screening* section on page 148, as its name implies, deals primarily with cargo other than baggage, in facilities that in some cases may be within the terminal or may be found at relatively remote locations both inside and outside the immediate airport boundaries. In the latter cases, screening may have additional operational and procedural requirements if, for example, screened cargo must then be transported from one secure area to another and perhaps stored for a period of time until loading and departure.

Security screening checkpoint (SSCP) requirements were established in 1973 to deter aircraft hijacking and improve the safety of the traveling public. These requirements were the responsibility of the aircraft operator to implement and ensure compliance with the regulations. Following the terrorist attacks of September 11, 2001, Congress established the Transportation Security Administration (TSA) and directed TSA to federalize passenger and checked baggage screening operations at most commercial passenger service airports. The passenger screening checkpoint is an essential component of the overall airport access control system, methods and procedures required by the Airport Security Program (ASP). When establishing the security areas of the airport, attention should be given as to how the checkpoint will be controlled during non-screening periods, which may affect the downstream control requirements as well as equipment needs and design. Refer to the *ACAMS* section on page 150 for further information.

In implementing this Congressional mandate, the Transportation Security Administration has developed extensive enhancements of the original design requirements to accommodate a broad range of new technologies and significant changes in the accompanying personnel requirements. A great deal of experience has been gained regarding layouts, equipment, operations, and how different designs facilitate or encumber appropriate reactions to security events.

TSA has revised the design criteria applicable to airport security screening checkpoints (SSCP), and the process of applying these criteria to determine SSCP capacity, personnel requirements and other operational parameters. Previously, when screening operations were conducted by airline personnel, the federal government's design criteria for the SSCP were made available to planning and design professionals, who performed the necessary computations to derive throughput, personnel, and space requirements. Since ATSA, TSA has specified design criteria at a greater level of detail, and considers some of these details Sensitive Security Information (SSI) subject to disclosure restrictions under 49 CFR 1520.

As a result, TSA no longer provides computational formulas to the public for use in determining SSCP throughput, personnel, or space requirements. Instead, TSA uses proprietary tools to determine these requirements. TSA provides the computed requirements to airport planners and designers for use in planning and designing airport facilities.

Computational formulas found in previous editions of this guidance document are no longer recommended, as they may no longer provide accurate results. (The former computational formulas are provided in *Appendix B* for historical purposes.) For purposes of roughly estimating the number of screening lanes required in early planning studies, the post 9 -11 throughput capability when fully loaded of passengers is currently at 175 to 250 passengers per hour per lane, and the rate continues to improve. (Designers and planners should realize that throughput may decrease or increase depending on changes in security protocols in response to external events.)

This section does provide revised and updated space layout diagrams for use by airport planners and designers; however, to plan or design a new or modified airport SSCP with confidence, the planner or designer is urged to consult early with TSA Federal Security Director (FSD) to obtain project-specific requirements and further guidance.

1. Passenger Security Screening Checkpoints (SSCP)

Over the past several years, a number of critically important checkpoint design elements have been identified and integrated to create a typical TSA Security Screening Checkpoint. This section is intended to provide some lessons learned from that experience, and to present ideas and technology that shape SSCP design. Planners, architects, and engineers should address a series of key questions:

- What issues need to be addressed in SSCP design?
- What regulation references are available for the design of SSCPs?
- Who are the key people to talk to in the design process?
- What elements of airport planning should be considered in determining SSCP location and characteristics, and how much space should be allocated for checkpoints?
- What are the component parts of SSCPs, how are they staffed, and how do they work?
- What are some examples of successful SSCP designs, and what ideas are being developed for the future?
- What funding is available to support the component parts of the SSCP?

This section will address these issues:

a. General Issues
b. Regulations and Guidelines
c. Essential Coordination
d. Planning Considerations
e. Elements of the SSCP
f. SSCP Operational Efficiency
g. SSCP Layout Standards
h. SSCP Spacing Requirements
i. SSCP Project Funding
j. Designing for the Future

a. General Issues

SSCPs are a critical element of airport terminal security design, and must be included in planning, design, and engineering considerations from the conception of the project, including early conversations with airport and airline representatives. TSA regulation documents, many of which are non-public, describe performance requirements of security screening checkpoints, including airport and airline responsibilities.

Security screening is intended to prevent hijacking and deter the carriage aboard airplanes of any explosive, incendiary, or a deadly or dangerous weapon. SSCPs provide screening of credentialed airport, airline and concession employees, concession delivery personnel, passengers and their carry-on or personal items. Non-ticketed visitors are currently not allowed beyond security. Non- ticketed visitors wishing to assist passengers to their gate must obtain approvals and documentation from the airline prior to entering the SSCP. Proper SSCP design helps avoid a host of problems for the airport and airlines, including terminal and queuing congestion, delays, and unnecessary security risks. Further, there is a need to design with an awareness of wheelchairs and other assistance equipment for the disabled.

Among the general issues to consider are:

- Cost-effectiveness for airlines, airports, and TSA.
- Deterrence of potential adversaries, both in terms of actual detection of contraband of any kind, and in creating the maximum perception of effective security measures.
- Effective and secure handling of goods and services other than individuals, required to cross from non-sterile area to sterile area;
- Efficient and effective use of space, allowing more space to be available for operational or revenue-generating uses.
- Flexibility to accommodate highly-specialized equipment that has constantly changing engineering requirements.
- Minimal interruption or delay to flow of air-travelers and others passing through the terminal from non-sterile public areas to sterile areas.
- Operational flexibility in response to changes in passenger load, equipment use, and operational processes, including the increasing use of electronic identification media.

- Prevention of unauthorized breach of exit lanes at SSCPs for entry into sterile areas.
- Coordination of HVAC, electrical, telecommunications and electronic components of the SSCP.
- Protection of SSCP integrity when the checkpoint is not in use.
- Space, including the possibility of office space, for IT equipment and work areas for TSA staff.

b. 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 technical requirements that govern design of SSCPs, they define in general terms what must be accomplished by the design. They also provide information about how other jurisdictions approach terminal security. Virtually all TSA regulations can be obtained on TSA web page, *www.TSA.gov*.

SSCP guidelines will continue to evolve as new security technologies are proven and incorporated. Prior to drafting SSCP plans, it is important that airports coordinate with both the local TSA Federal Security Director (FSD) and TSA Aviation Operations in Washington, DC to review guidelines for the design of Security Checkpoints. The airport, as a public institution that is part of a city, state or other governmental entity, may have additional security, construction or code requirements other than those mandated by TSA.

c. Essential Coordination

Key individuals in TSA, airport and airline operations personnel should be consulted at various stages of the SSCP design process. The airport is subject to local, city and state building codes, mutual aid agreements with local law enforcement and emergency responders, and may be party to other arrangements, such as or a joint military presence on the airport, that could strongly affect all areas of security design.

TSA requires all checkpoints to be formed as collections of single and double-lane team modules as illustrated in "SSCP layouts." Modular design enables a controlled and contained screening environment where "sterile" and "non sterile" passengers and baggage are separated from each other. Whenever possible, allowances should be made for flexibility and expandability of the checkpoint space to respond to changes in technology, equipment or processing.

The location of the SSCP relative to concessionaires and other airport services should be resolved early in the process through conversations with the airport representative, as this will affect airport operations and revenue.

d. Planning Considerations

Each airport and airport terminal building is unique in terms of physical conditions and operational requirements. Therefore, no single SSCP solution will work for all airports, or possibly even among multiple locations within the same airport. This section discusses where and how large an SSCP should be for a variety of conditions.

The location and size of the SSCP depends, among other things, on the type of risk that is present or anticipated, the type of operations at the airport, the passenger loads, and the character of the overall design of the airport.

1) Level and Type of Risk

Airports with international flights support complex operations and may be seen as being at a somewhat higher level of general threat than purely domestic airports. The result may be more types of equipment and greater staffing in the SSCP and elsewhere, with the resulting need for more space.

Airports in rural or less densely populated areas may require simpler equipment and less space and staffing due to the lower passenger loads and lower throughput. However, the designer should not be

misled into believing that lesser levels of security are therefore appropriate, as all airports represent points of entry into the aviation system, and must meet minimum criteria. Future planning may also dictate an expandable design.

Some specific local vulnerability may affect the decision for a location of the SSCP. Some airports may install a permanent zone of security screening at or near the entrance wall of the terminal, so that all interior spaces beyond that point are sterile. The more typical choice is to allow unscreened access further into the terminal, but may require that space and utility connections be available for temporary installation of SSCPs at the entry of the terminal during periods of elevated threats. If the SSCP is implemented close to an entrance wall, thoughtful consideration must be given to SSCP queuing to avoid creating a target by massing people in public areas.

2) Operational Types

Airports can be characterized as Origin and Destination (O&D), Transfer/Hub, or a combination of the two, with regional and commuter traffic participating in all three.

In Transfer/Hub operations, transfer passengers frequently move from gate to gate without passing through the airport's SSCP. If concessionaires are in the sterile area, this pattern is reinforced. If the main concession is in the non-sterile public area, there may be an incentive for passengers to exit the sterile area and subsequently reenter through the SSCP, burdening it with added traffic that might otherwise be unnecessary.

Transfer/hub operations benefit from an SSCP that is located so that passengers can move among gates along multiple concourses without being re-screened. On the other hand, O&D operations may benefit when SSCPs are located near individual hold rooms and only staffed for individual departures. Very small airports often screen directly before boarding a flight, and provide little or no hold room space; these SSCPs may be located directly at the door to the airside.

3) Location of SSCPs (Relative to operational type)

Three basic types of SSCPs can be identified, related to their operational type. The two in widest use in the United States are the Sterile Concourse Station SSCP and the Holding Area Station SSCP.

a) The Sterile Concourse Station SSCP plan (refer to *Figure III-E-1 below*) is usually considered the most desirable from the standpoint of passenger security and economics. It is generally located at the entry to a concourse or corridor leading to one or more pier(s) or satellite terminal(s) and permits the screening of all employees, passengers, visitors and deliveries passing through the SSCP. This configuration is well suited for transfer operations. It can control access to a considerable number of aircraft gates with a minimum amount of inspection equipment and personnel. Pier and satellite terminal layouts are well suited for the Sterile Concourse Station SSCP; this configuration enables connecting passengers to move between concourses and among concessionaires without leaving the sterile area, and without being subjected to multiple screening processes. In general, the more individual SSCP locations that serve multiple locations within an airport, the more redundancy required in each to handle their individual peaks. The "centralized" approach in this example can facilitate efficiencies in staff and equipment deployment.

On the other hand, in the event of a security breach, locating and isolating the suspect may be difficult, since the single large sterile area then contains the entire screened population. In extreme cases a security breach may lead to total airport shutdown. Zoning the building into areas that can be closed off in the case of a security breach can mitigate this.

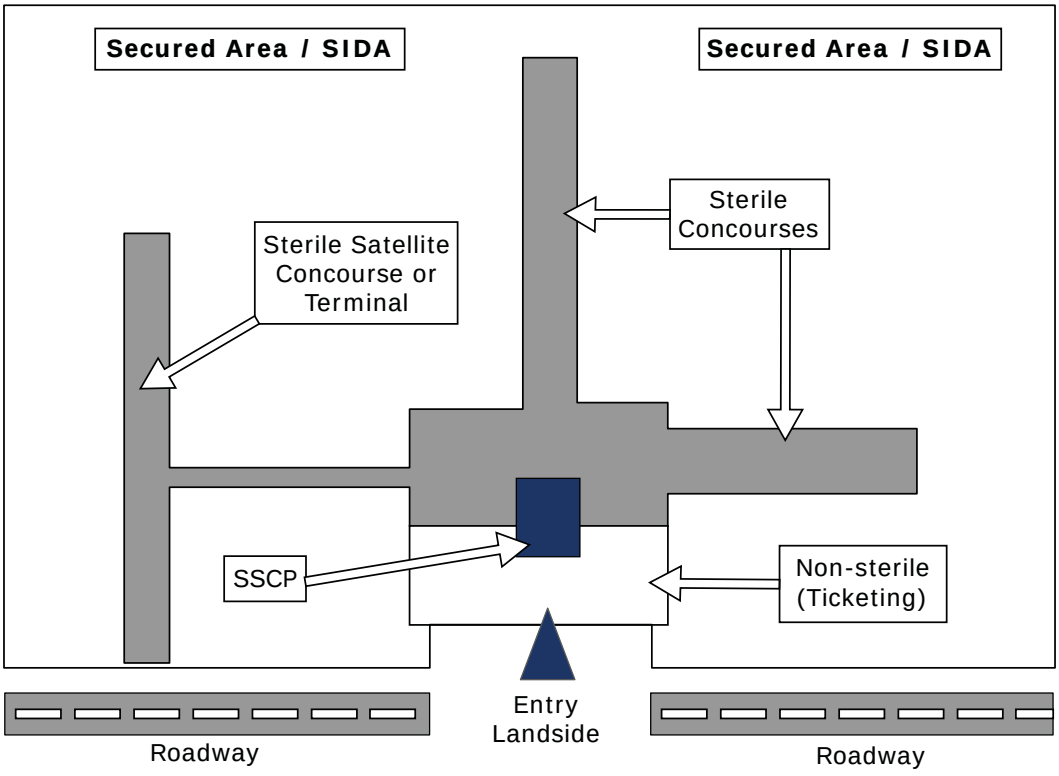


Figure III-E-1 - Sterile Concourse Station SSCP

b) In the Holding Area Station SSCP plan (refer to *Figure III-E-2* below), screening is carried out at the entrance to an area designed to hold passengers awaiting a specific flight. Walls or suitable barriers usually define this area, and access points must be appropriately controlled. Access portals from this area to aircraft loading walkways or ramps must remain locked or monitored until boarding begins, by which time inspection or screening of passengers and carry-on baggage has been completed. Holding Area Station SSCPs must be secured when not in use to ensure sterility is maintained; if that is not possible through design, then the hold area must be searched prior to use. While the Holding Area SSCP plan may require staffing only during the screening process, multiple hold areas will require multiple staffing. In case of a security breach, restoration is relatively easy in the Holding Area Station SSCP plan, and operations at other gates/hold rooms will not be affected. This plan is more likely to benefit small airports with fewer gates and limited screening requirements.

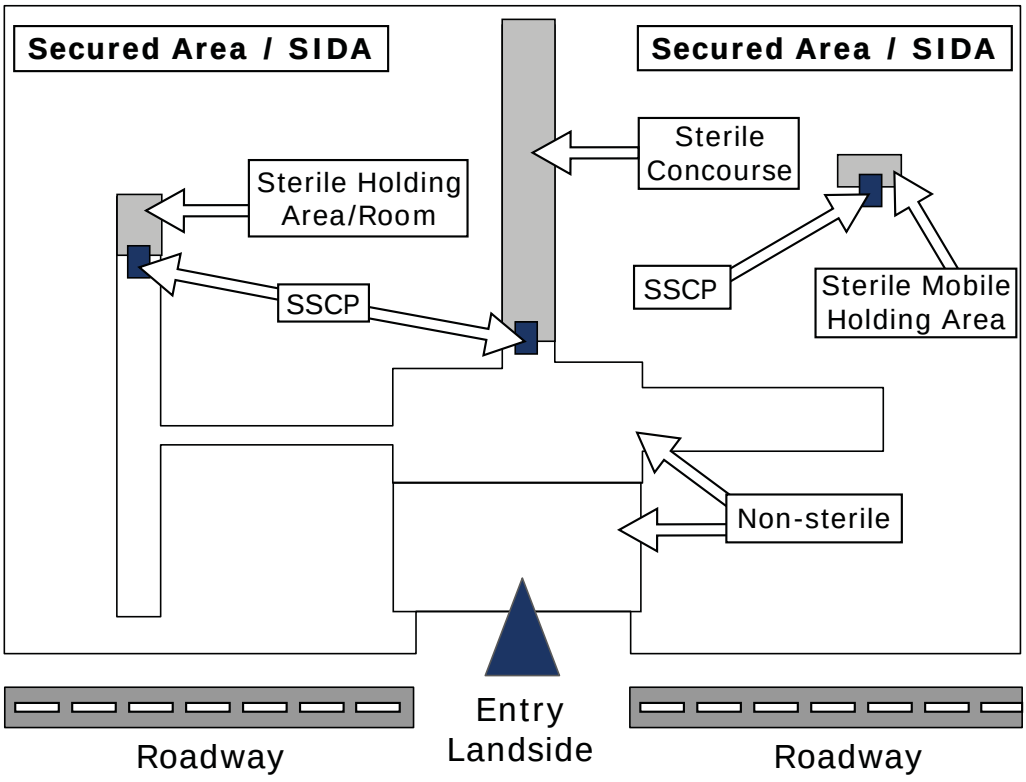


Figure III-E-2 - Holding Area Station SSCP (O&D)

c) The Boarding Gate Station SSCP plan (refer to *Figure III-E-3* below), more commonly utilized by small regional airports, features the screening of passengers and their belongings immediately before boarding at a station established at the gate(s) leading to an aircraft. In this case, the gate may be a door leading to an aircraft loading walkway or to a ramp area where the aircraft is parked. Boarding Gate Station SSCPs need be staffed only while screening is in progress but must be secured when not in use. This approach may be beneficial to smaller airports with limited screening requirements. Another advantage of this plan is that it affords the least opportunity for the surreptitious transfer of weapons or dangerous devices to passengers after screening.

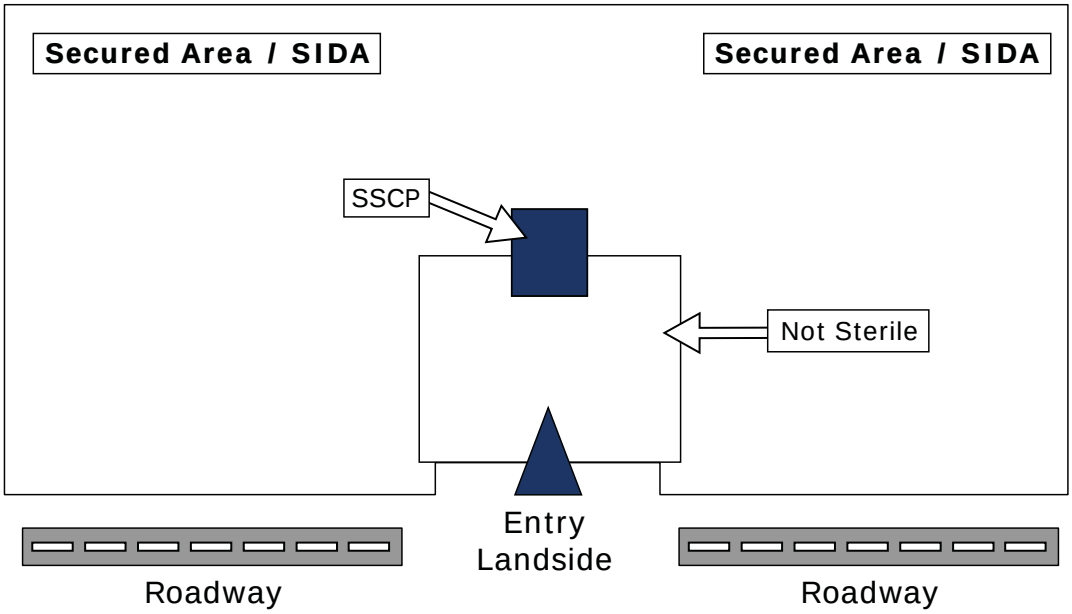


Figure III-E-3 - Boarding Gate Station SSCP (Small Airport)

4) SSCP Size

While vulnerability assessments and operational characteristics, including level of service, play a large role in determining the location of SSCPs, it is the current and anticipated passenger load that ultimately provides the specific information with which the SSCP can be sized and designed.

For general planning purposes, except at very low activity airports where manual search procedures may be employed, an SSCP will generally include a bare minimum of one walk-through metal detector and one x-ray device.

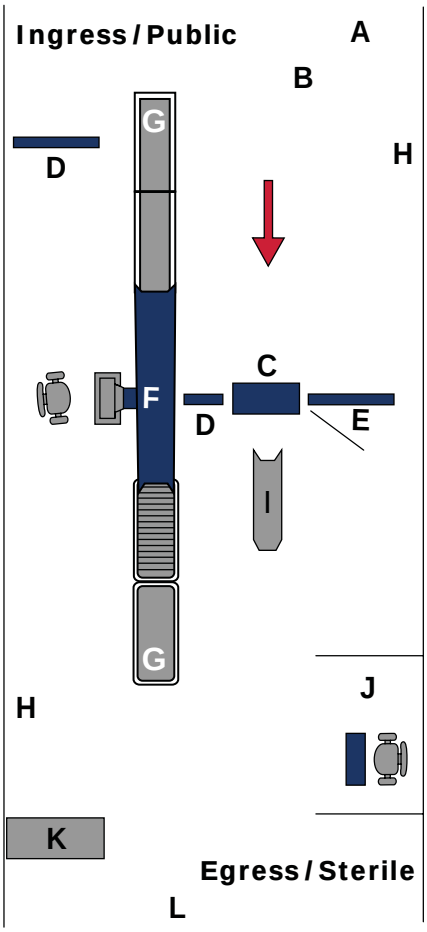
e. Elements of the SSCP

SSCPs are usually made up of elements that are similar from one installation to the next, whether they are pieces of equipment or areas of floor space required for the operator to function or for pedestrian flow. The size of some elements is nearly universal, such as metal detectors; some can be highly variable, such as space for queuing, which varies with load factors and throughput. The intention of this section is to provide a checklist of items that the designer will need to consider in an overall SSCP design. Full SSCP layout diagrams are provided in item 5 "SSCP Layouts" that illustrate options for how each of these elements will be located. Please note that Designers and Planners may suggest preferred equipment choices, however the TSA will make final determination for each installation. *Table III-E-1* below indicates the standard elements of a TSA checkpoint.

Table III-E-1 - Elements of a Standard TSA Checkpoint

Checkpoint Area	Equipment Elements
Per Single Lane	(1) Enhanced Walk Through Metal Detector (WTMD) (1) Carry-On Baggage X-Ray with roller extensions
Per Module (1 or 2 Lane)	(1) Explosives Trace Detection (ETD) machine (1 or 2) Bag Search Tables (1) Glass Wanding & Holding Stations (1 or 2 sides)
Per Checkpoint	(1) Law Enforcement Officer (LEO) Station or position (1) Supervisor Station (at larger airports only) (1) Private Search Area (0 2) SupplementalX-ray 1 or 2 lanes: None 3 to 5 lanes: One 6 or more lanes: Two (1) Data Connections/Cabinet

Conceptual drawing *Figure III-E-4* below underscores the point that all elements of the system, no matter how seemingly insignificant require an allocation of dedicated space. The following diagram shows typical elements that may be part of the screening process in the direction (top to bottom) that an individual moves from non-sterile to sterile areas:



Legend (Letters refer to those within the diagram and the following paragraphs):

A = Prescreening Preparation Instruction Zone
B = Queuing Space
C = Walk Through Metal Detector
D = Non Metallic Barrier
E = Non Metallic ADA Gate
F = Carry-on Baggage X-ray Machine
G = Divest & Composure Tables
H = SSCP Adjacent Walls/Barriers
I = Holding Station
J = Wanding Station
K = Explosives Trace Detection (ETD) Machine with table
L = Egress Seating Area

Other elements (not shown in this diagram):

Explosive Trace Portal
Supplemental X-ray
LEO Station
Supervisor Station
Private Search Area
SSCP CCTV Coverage
Data Connections / Cabinet
SSCP Lighting
Wireless Access Point
Exit Travel Lane
Exit Lane Station
Exit Lane CCTV
Integrated Exit Lane Systems

Figure III-E-4 - Typical SSCP Layout and Elements

1) **A - Prescreening Preparation Instruction Zone** (Refer to *Figure III-E-4* above)

   This zone is an area in front of the SSCP that uses architectural features, simple signage and instructional videos, and "ambassador" staff to create a calming atmosphere and more efficient throughput by instructing and directing passengers for efficient screening flow.

2) **B - Queuing Space** (Refer to *Figure III-E-4* above)

   An appropriate space allocation should be made on the non-sterile (public) side of the checkpoint for passenger queuing. This space should include room for tables near the screening equipment, for preparing their belongings for screening. Emphasis on efficient queue management, passenger education and divestiture in this area will greatly improve the efficiency of operations for all. Note that staff-support amenities such as a coatroom or lunchroom are in addition to the size requirements developed from passenger loads, and are generally located away from the SSCP.

   SSCP layout can affect the queue dramatically. When evaluating queuing space, TSA suggests estimating 9 SF per passenger. In designing the layout of the queue, be aware of specific path of travel conflicts: the queue should not interfere with other traffic patterns. In some airports an attended station before the queue may be used to check for tickets if only ticketed passengers are allowed into the queue.

3) **C - Walk Through Metal Detector (WTMD)** (Refer to *Figure III-E-4* on page 95)

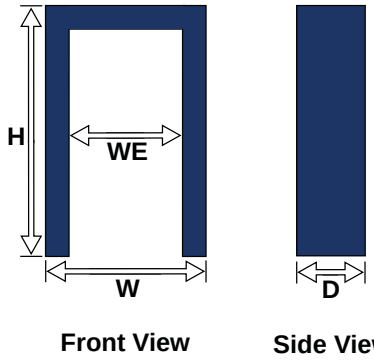
Over the past few years, TSA has upgraded all earlier WTMDs to an "enhanced" status. During this transition, TSA referred to the earlier devices as WTMDs and to the newer devices as Enhanced Metal Detectors, or EMDs. Now that all the deployed devices have been upgraded to "enhanced" status, all deployed metal detectors are referred to as WTMDs.

The WTMD is a walk-through arch for detection of metallic items carried by the individual. With the deployment of the latest metal detector technology, there are a number of placement requirements that must be taken into account to minimize environmental and equipment interference:

- The WTMD should be aligned next to the center of the EDS chamber, equidistant from both the ingress and egress points of the chamber.
- The sides of the WTMD should be given a 12" to 15" clearance from all other equipment, walls, or columns located in the checkpoint. Certain factors can interfere with WTMD operation and should be considered when determining the design surrounding the desired WTMD location:
- Electrical fields from escalators, conveyor belts, neon fixtures, transformers, banks of electrical circuit breakers, power cables, conduit, speakers, etc., both overhead and below the floor.
- Metal from surrounding architecture, including doors, metallic framing, wall support studs, facade systems, etc.
- Surface vibrations created by equipment above, below or immediately adjacent to the checkpoint, including baggage conveyors, subway trains and heavy truck traffic.
- The plugs for WTMDs should be secured using twist-lock receptacles. Emergency or backup power is not required at this time for checkpoint areas.

Upon installation, WTMD machines will be bolted or otherwise secured to the floor. Currently, only the original equipment manufacturer (OEM) is certified to recalibrate these machines; consequently, WTMDs cannot be moved by anyone except the manufacturer. Typically, TSA will deploy different manufactures' equipment based on compatibility with existing checkpoint equipment.

Refer to *Figure III-E-5* below and *Table III-E-2* on page 97 for information on WTMD dimensions and currently approved models.



Width (W):	Allow 33″ to 37″
Depth (D):	Allow 23″ to 26″
Height (H):	Allow 86″ to 88″
Width Entry (WE):	28 to 30
Weight:	Approx. 100 lbs.
Power:	110 VAC, 30 to 55 watts

Figure III-E-5 - Typical WTMD Dimensions

Table III-E-2 - Currently Approved WTMDs

Manufacturer	Model	Width	Depth	Height	Width Entry	Height Entry	Power (110vac)
CEIA	02PN20	32.75″	26″	87.5″	28.25″	80.75″	30 watts
Garrett	6500i	35″	23″	87″	30″	80″	55 watts
Metorex	200HDe	36.2″	23.4″	85.7″	30″	79.2″	45 watts

4) **D - Non-Metallic Barriers** (Refer to *Figure III-E-4* on page 95)

Barriers must be installed to close any gap exceeding 15" across the front width or façade of the checkpoint, to prevent people and items from passing into the sterile area without also passing through either an ETP machine or Walk Through Metal Detector. These barriers should be primarily non-metallic and rigid enough to prevent vibrations that could interfere with the WTMD. Barriers must extend from the floor a minimum of 48" high, and be self-supporting to alleviate any potential tripping hazards. It is recommended that barriers be constructed primarily of transparent material. Standard barriers come in 2', 3' or 4' widths, but may also be custom designed. Refer to *Figure III-E-6* below.

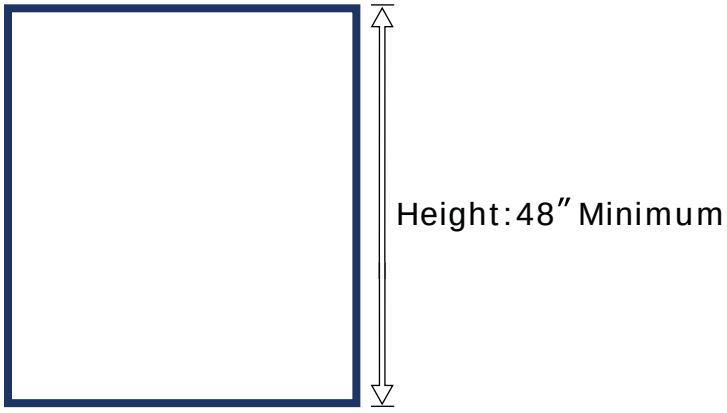


Figure III-E-6 - Non-Metallic Barrier

5) **E - Non-Metallic ADA Gate/Access** (Refer to *Figure III-E-4* on page 95)

Access for disabled passengers through the checkpoint screening process must be provided. As WTMDs are typically not wide enough to meet Americans with Disabilities Act (ADA) requirements, a gate or other passageway must be provided next to at least one WTMD so passengers in wheelchairs can be directed into the wanding or holding station. Limited use of metal should be considered when designing/fabricating this gate because of the tendency to interfere with adjacent WTMDs.

When planning new checkpoint construction and design, the use of an exit lane for wheelchair access to the sterile area is not acceptable. ADA exit lane access or the use of any special ADA passageways must be defined during the initial planning engagement effort. The swing direction of the ADA gate should conform to local codes. Most approved ADA gates are 45" wide, with a 36" interior swing gate made of non-metallic, primarily transparent material.

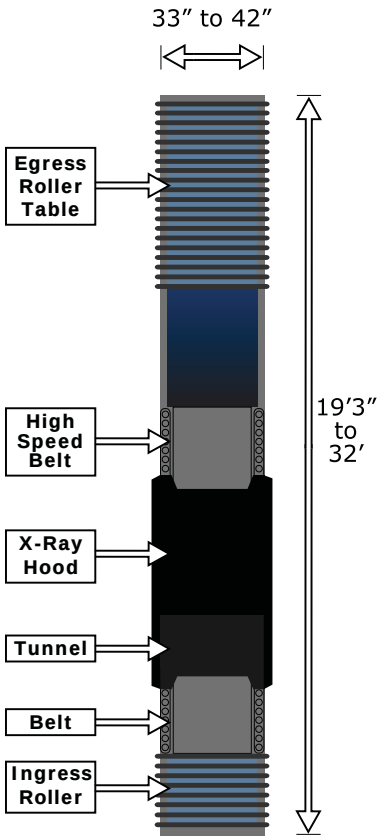
6) **F - Carry-On Baggage X-ray Machine** (Refer to *Figure III-E-4* on page 95)

Space requirements for x-ray machines include space for loading bags onto the conveyor, area for x-ray equipment, area for the operator, area for the conveyor exiting the equipment; and areas for secondary inspection. The x-ray machine is one of the largest and heaviest components of the SSCP. Floor structure must be provided or reinforced to support the weight, and electric power must be provided.

Video monitors are typically mounted to assist an operator in controlling the rate at which the images flow by. Interpreting the monitor information requires concentration. An ergonomic, distraction-free environment for the screener is highly desirable. Interior lighting should be designed to avoid screen glare on monitors, and the operating space should be designed so that bright sunlight through windows does not wash out or produce glare on monitors.

The exit conveyor often has two sections, a slow-running section just exiting the x-ray, and a faster conveyor to carry bags to where they will be retrieved by the passenger. A faster and longer second-section conveyor can put bags further past the metal detectors, since people tend to congregate where the bags stop moving, impeding flow. In general, the location at which bags from the x-ray machine end up should be planned carefully in relation to overall flow issues, especially where people will exit primary and secondary row metal detectors. Egress extension rollers can be added; they are currently available in 3'-3", 4'-0" and 6'-0" lengths depending upon manufacturer.

Refer to *Figure III-E-7* on page 98 and *Table III-E-3* on page 99 for information on X-Ray dimensions and currently approved models.



Width	Allow 33″ to 42″
Length	Allow 19′ 3″ to 32′ Pending equipment type & conveyor sections.
Height	Allow 50″ to 55″
Weight	880 lbs- 1,380lbs. Allow 1,400 lbs, on four casters for tunnel and conveyors.
Tunnel Size	24″ to 30″ W x 16″ to 22″ H
Power	Standard 110 V, 60 Hz, 15 amp line; power cord is under exit conveyor on back end of machine. EDS and metal detector should be on different circuits or phases to avoid harmonics.

Figure III-E-7 - Standard Size and Layout of an X-Ray Implementation

Table III-E-3 - TSA-Approved Carry-On Baggage X-Rays

Manufacturer	Model	Length w/o roller	Width	Height	Weight (lbs)	Tunnel Size (W″ x H″)	Power (110 VAC)
Smiths Heimann	7555i	83.5	39.2	56.8	1279	29.5 x 21.7	????
Smiths Heimann	6040i	78.9	33.5	50.6	882	24.2 x 16.1	????
Rapiscan	520B	102.0	33.1	53.0	1232	25.2 x 16.9	10 amps
Rapiscan	522B	109.5	41.3	58.1	1367	29.5 x 21.6	10 amps

7) **G - Divest & Composure Tables** (Refer to *Figure III-E-4* on page 95)

Divest and composure tables are tables onto which a person divests personal items before they enter the x-ray, and from which the passenger retrieves personal items after they have been x-rayed. These tables currently come in 4'-0" and 6'-0" lengths and should be considered for their added value of throughput efficiencies at all lanes. Lanes that do not have a least one divest and composure table combined, have the potential for added delay while the passenger divests or composes. TSA strongly recommends at least two divest tables aligned directly to the in-feed belt of the x-ray and one composure table that is flush to the egress extension rollers.

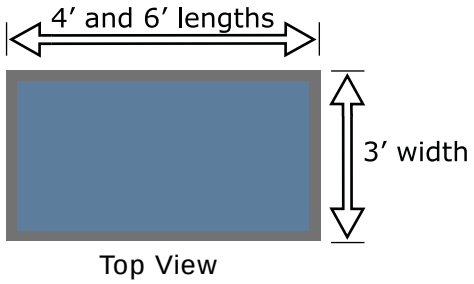


Figure III-E-8 - Typical Divest and Composure Table

8) **H – SSCP Adjacent Walls/Barriers** (Refer to *Figure III-E-4* on page 95)

Walls surrounding the security checkpoint must be a minimum of 8' high. Ideally, walls that separate sterile areas from non-sterile areas should be floor to ceiling, and designed without gaps such that no prohibited items could be placed into the secure side of the terminal when the SSCP is closed. Exit lane walls adjacent to the checkpoint are to be 8' minimum and constructed of transparent material where possible. Where possible, walls or other barriers adjacent to x-ray operators should prevent public view of the x-ray monitor screen.

9) **I - Holding Stations** (Refer to *Figure III-E-4* on page 95)

A holding station differs from a wanding station in that it is created specifically to hold passengers temporarily until screeners are available to escort them to the proper area to conduct secondary screening.

The holding station must be positioned so passengers can be diverted directly into the area without obstructing the path of non-alarming passengers, and must prevent the passing of prohibited items to sterile passengers.

Holding stations should be a minimum of 8’ in length and 3’ in interior width Up to three passengers can be held simultaneously in an 8’ configuration.

Holding Station walls shall be designed and constructed per the wanding station criteria outlined in *Figure III-E-9* below.

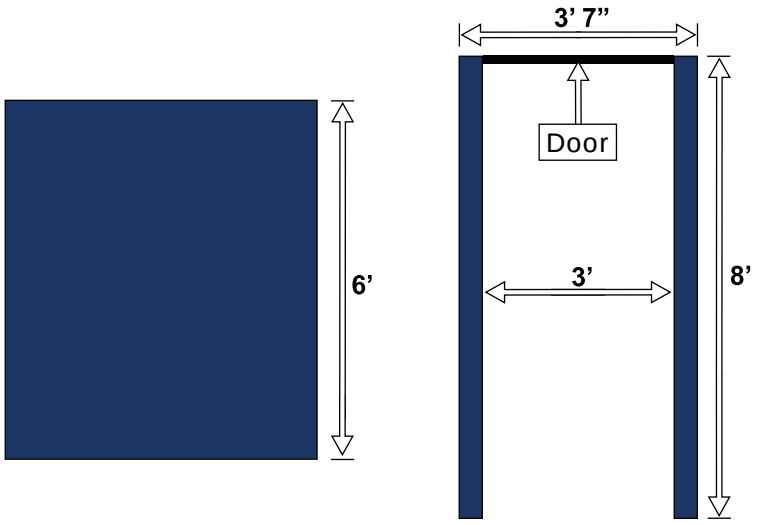


Figure III-E-9 - Typical Holding Station

10) **J - Wanding Stations** (Refer to *Figure III-E-4* on page 95)

Wanding stations are used to separate passengers who have alarmed the WTMD and/or require additional screening via a Hand Held Metal Detector (HHMD or "wand"). Such stations must prevent the passing of prohibited items to sterile passengers. The station must be positioned so passengers can be diverted directly into the area without obstructing the path of cleared passengers.

Refer to *Figure III-E-10* below for layout and dimension information.

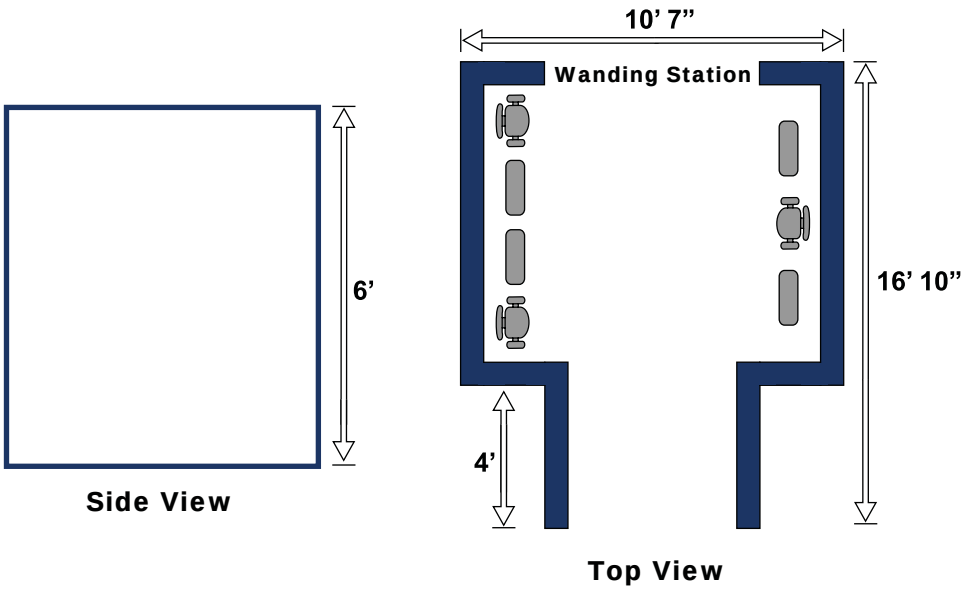


Figure III-E-10 - Typical Wanding Station

Wanding stations should include a minimum of a 4' long entry channel to allow queuing space for passengers waiting to be screened. Without this "waiting area," the main screening lanes would need to be halted whenever the wanding station filled.

Up to three passengers can be screened simultaneously in the typical configuration as illustrated in the wanding station diagram above. For width-constrained checkpoints, the 2 or 3 -passenger wanding station can be modified to a linear configuration. In addition to the 4' long neck, a linear configuration requires 6' of length per passenger and 7' of width to ensure operability.

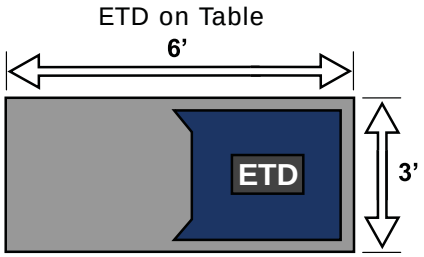
Wanding station walls should be fastened flush with the floor and be 6' high. The structure must be self-supporting to eliminate the need for structural supports that may pose tripping hazards to passengers. Wanding stations should be constructed primarily of transparent materials so passengers can maintain visual contact with their baggage. The amount of metal, particularly steel, within the structure should be minimized to reduce interference with the HHMDs. Most wanding stations include reinforced corner brackets, solid aluminum top cap, and have bottom kick plates. The length and type of anchor bolts should be suitable to the local floor conditions. Wanding station walls may be custom designed to these criteria, or obtained from TSA approved manufacturers.

Exit doors from the wanding station on the sterile side are strongly suggested, and should be designed to contain passengers until screening is completed.

11) **K - Explosives Trace Detection (ETD) Machines** (Refer to *Figure III-E-4* on page 95)

Explosives trace detectors (ETDs) are generally placed upon 6' (L) x 3' (W) standard stainless steel-topped tables consisting of two elements: an open bag search area and a protective hood surrounding the ETD. Two-piece tables are also available. The location of ETD's should support two lanes and be located out of the natural flow of exiting passenger traffic to prevent accidental placement of passenger bags on the ETD table.

Refer to *Figure III-E-11* and *Table III-E-4* below for information on ETD dimensions and currently approved models.



ETD Machine Size

Width	15.5″ to 28.5″
Depth	13.5″ to 29″
Height	13″ to 18.5″
Weight	(not a structural concern)
Power	110/220 VAC; DC power available

Figure III-E-11 - Typical ETD Machine Layout

Table III-E-4 - TSA-Approved ETD Machines

Manufacturer	Model	Width	Depth	Height	Power (110 VAC)
Smith (Barringer)	Ionscan 400B	15.5″	13.5″	13	6 amps
GE Interlogix (Iontrack)	Itemiser 2-Windows				????
Thermo Electron	Egis II	28.5″	29″	18.5″	????

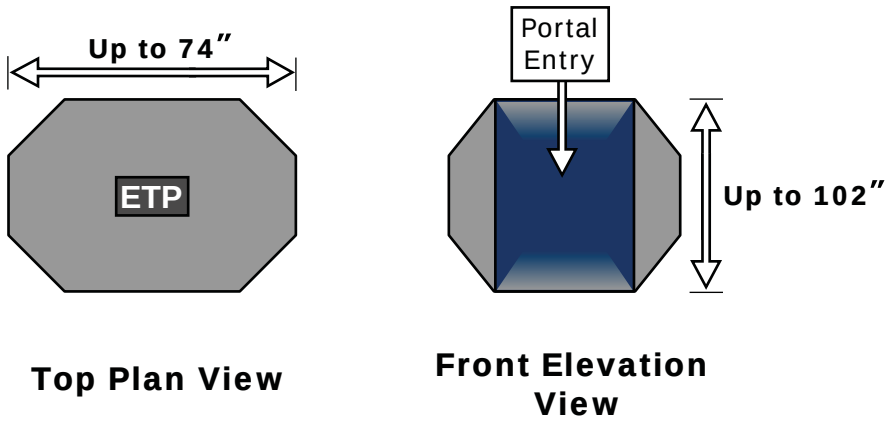
12) **L -Egress Seating Area** (Refer to *Figure III-E-4* on page 95)

Planners and designers should allow for sufficient floor space to accommodate a seating area after the passenger completes a screening process. This area may be after each lane, module or combination thereof; passenger safety and flow should be considered with the location of any seating.

13) **Explosive Trace Portal**

The Security Explosive Trace walk-through Portal (ETP) enables the detection of a broad spectrum of concealed explosives. This device is similar to the metal detector in terms of walking through an arch. However, it requires the person being "searched" to pause in the archway. The ETP machine can be one of the heaviest components of the SSCP. Floor structure must be provided or reinforced to support the weight, and electric power provided. An air compressor is a key component of the ETP and depending on the manufacturer; the compressor may be physically separate from the unit itself. Dimensions, weight and power requirements vary.

Refer to *Figure III-E-12* below for information on ETP dimensions.



Dimensions	H=102″ x W=48″ x D=40″ to H=90″ x W=74″ x D=55″
Weight	Approximately 631 lbs to 1775 lbs.
Power requirements	208/230 VAC, 50 Hz or 60 Hz / to 208/220 VAC, 50 Hz or 60 Hz / 40 A maximum
Compressor	30 A, 120 VAC

Figure III-E-12 - Space Required for Typical ETP

Allow a minimum of 18" clearance on each side of ETP for service and maintenance functions and a minimum of 6" on top for proper airflow.

14) Supplemental X-ray

Currently, supplemental x-rays (refer to *Table III-E-5* below) are deployed at checkpoints having three or more lanes to screen shoes and other items during the secondary screening process, to enhance throughput at the largest checkpoints. Supplemental x-rays should be positioned at the rear of the checkpoint such that they can be easily accessed from wanding and holding stations. These machines are dramatically smaller than standard carry-on baggage EDS machines and are not certified for carry-on baggage screening.

Table III-E-5 - TSA-Approved Supplemental X-Rays

Manufacturer	Model	Length w/o roller	Width	Height	Weight (lbs)	Tunnel Size (W x H)	Power (110vac)
Smiths Heimann	6030di	68″	31.4″	42.5″	725	24 x 12.6	???
Smiths Heimann	5030S	47.2″	27″	25″	276	20.9 x 12.6	???
Rapiscan	519	61.2″	31.2″	52.6″	690	20.5 x 12.6	6 amps
L3 Linescan	222	48.2″	30.6″	27.5″	496	20.5 x 12.9	10 amps

15) Law Enforcement Officer Station

A law enforcement officer (LEO) station may be positioned at the rear (sterile side) of the checkpoint to enable the LEO to view the entire screening operation. Positioning so the LEO has an unobstructed view of as much of the checkpoint as possible is critical to the LEO's ability to identify and respond to situations that may develop in the checkpoint. After working with the FSD, there are alternatives to having an LEO at the SSCP.

16) Supervisor Station

The Checkpoint Screening Supervisor (CSS) should have access to a workspace – a podium at a minimum – positioned at the rear of the checkpoint to enable the CSS to view the entire screening operation. If there is an LEO position, the CSS can be adjacent.

17) Private Search Areas

A private search area must be made available to accommodate passengers who request a private search. This area should provide complete privacy and sufficient space, at minimum, for one passenger, two screeners, a chair and a search table. The private search area can be either a modular paneled system or an adjacent private room. In some limited cases, a curtain may be used.

18) CCTV Coverage

Cameras can increase the public's sense of security, deter burglary, and capture visual records of security activity, including breaches. In this type of application, correct placement of one or more cameras in the SSCP area is critical. For example, a camera that can only show the back view of a person breaching the SSCP is of very limited value, as opposed to a camera that displays a person's face and other identifying characteristics. Additionally, CCTV can monitor unmanned SSCP and adjacent areas for greater security.

19) Data Connections/Cabinet

Connections must be provided to connect security equipment to LANs, phone lines, and remote screening rooms, and from equipment to the CSS desk and to other selected points in the airport. Eventually, data from all screening equipment and trace machines will be collected automatically. Many airports undertaking new construction may install an information infrastructure, to which the SSCP data may be linked. The security infrastructure may be a separate system from the data infrastructure, protected by firewalls.

20) SSCP Lighting

Lighting in new/renovated security checkpoints areas should meet local code requirements, and ideally will meet the Occupation Safety & Health Administration (OSHA) 30fc requirement. The minimum lighting level should be 20fc or local building code if greater.

21) Wireless Access Point

Data and power outlets for a wireless data point should be positioned, where possible, at a central point with line-of-sight to the checkpoint and queuing area. Outlets should be a minimum of 8 feet above the floor or in the ceiling, with the ceiling being the preferred location. The associated electrical duplex and data jack should be co-located when possible. There should be one wireless access point for each checkpoint (not each lane). The wireless protocol or model of the wireless devices has not been specified by TSA at this time.

22) Exit Travel Lane

A travel lane should be adequately sized for deplaning traffic flow exiting the concourse. This lane must be sized to meet building code egress path width requirements. The location and size of the exit travel lane should be considered carefully to support good flow, clear way finding, and enhanced security.

Some airports have incorporated special measures, such as revolving doors or turnstiles, capable of blocking entry from the public side while permitting egress for those departing the sterile area, although this must also allow sufficient space for the passage of the person with baggage, and accommodate the disabled.

Control and design of travel and exit lane areas may be affected by the party or element having operational responsibility to ensure unauthorized entry into the area does not occur. The requirements may vary if it is the airport operator, air carrier or TSA which has total or shared control.

23) Exit Lane Station

An exit lane station is an area, often equipped with a table and chair or podium, for a security person to monitor and deter people attempting to bypass the SSCP by entering the sterile area from the public side through the exit lane. The security guard should be located to intercept traffic moving in pass-on-the-right patterns typical in the United States.

24) Exit Lane CCTV

Cameras are increasingly used to monitor the approach of pedestrian traffic attempting to enter the secure area through the exit lane. Some camera systems are programmed to record all traffic and to send recently recorded information to predefined monitors if a breach alarm is activated.

25) Integrated Exit Lane Systems

As in the non-sterile to sterile movement components, there are integrated systems available for exit lanes. These allow video cameras, sensors, and video monitors, with supporting architectural elements, to be integrated into the overall SSCP systems, with centralized control.

f. SSCP Operational Efficiency

Good layout designs support screening efficiency. For example, designs should place the x-ray operator in a position to concentrate on their computer monitor without distraction by persons going through the SSCP. This position should not be easily approachable for questions or conversation by people other than fellow screeners.

Similarly, the x-ray machine screener should not be located adjacent to a bypass lane, to further forestall distraction. Please note that the design team may recommend a preferred layout, however the TSA must approve the final configuration for each installation.

1) Designing for the Process

Good design should conform to the activity that it supports. Procedures are in place and being further refined that outline the process that every person and bag must undergo in order to properly fulfill the goals of the SSCP. It is critical that the SSCP layout support this process. SSCP layout should

respond to the fact that divesting and placing items on the belt are each discrete activities that take a certain amount of time. They are also activities that should begin well before the person to be screened reaches the WTMD or ETP.

The designer may consider conveyor belts with a somewhat longer "presentation length" on the non-sterile (public) side, to allow more time and space for people in line to begin placing bags on the belt.

2) Length of Response Corridor

Downstream of the SSCP, a length of hallway may be dedicated to detection and detention of persons attempting to breach the SSCP. In some earlier designs, the SSCPs were located close to boarding gates. Where these situations exists, consider adding see-through barriers between the SSCP and the gate, such as a substantial plastic or laminated glass wall or offset panels, so the SSCP can be observed to facilitate an immediate LEO response to an alarm. In new facility planning and design, consider separating boarding gates from the SSCPs to provide adequate time for response to a breach of the SSCP. The area might also incorporate CCTV surveillance so that breaches may be monitored until the incident is resolved.

In all cases, breach alarms should be installed both at existing SSCPs and wiring at locations that may be designed to house future SSCPs. In this way aircraft, especially those located at more distant gates, can be quickly protected by the immediate closure and locking of access doors and loading bridges upon alarm, and avoid delays resulting from a need to re-screen passengers or to conduct extensive security sweeps of the entire concourse/pier/terminal.

3) Architectural Design to Support Intuitive Processes

Architectural materials and lighting can play key roles in encouraging the successful operation of the SSCP. A floor color or material, for example, creating a large "entrance mat" ahead of the WTMD on the public side can clearly mark the area that is intended for queuing. By using a different floor material or color in front of the exit lane, it may become more intuitive to those on the non-sterile side that they are not supposed to go through the exit lane. Other material, spatial, or lighting clues may be used to reinforce the appropriate paths throughout the SSCP.

4) SSCP Signage

Simple and effective signage can be used to direct and instruct users of the SSCP, increasing the speed and perception of service. Signage should be kept very simple and should be integrated and approved relative to the airport's signage policy. Video monitors may be used to illustrate prohibited items, divesting, loading bags on the conveyor, and walking through the metal detector.

5) Space for TSA Staff

Accommodation should be made for TSA staff space, both for storage of personal items and for breaks. This area should not be accessible to the public.

g. SSCP Layout Standards

The following section shows typical TSA Airport Checkpoint Design Layout Standards.

These SSCP examples facilitate procedures in an orderly, consistent manner, reducing mistakes and enhancing supervision and customer satisfaction.

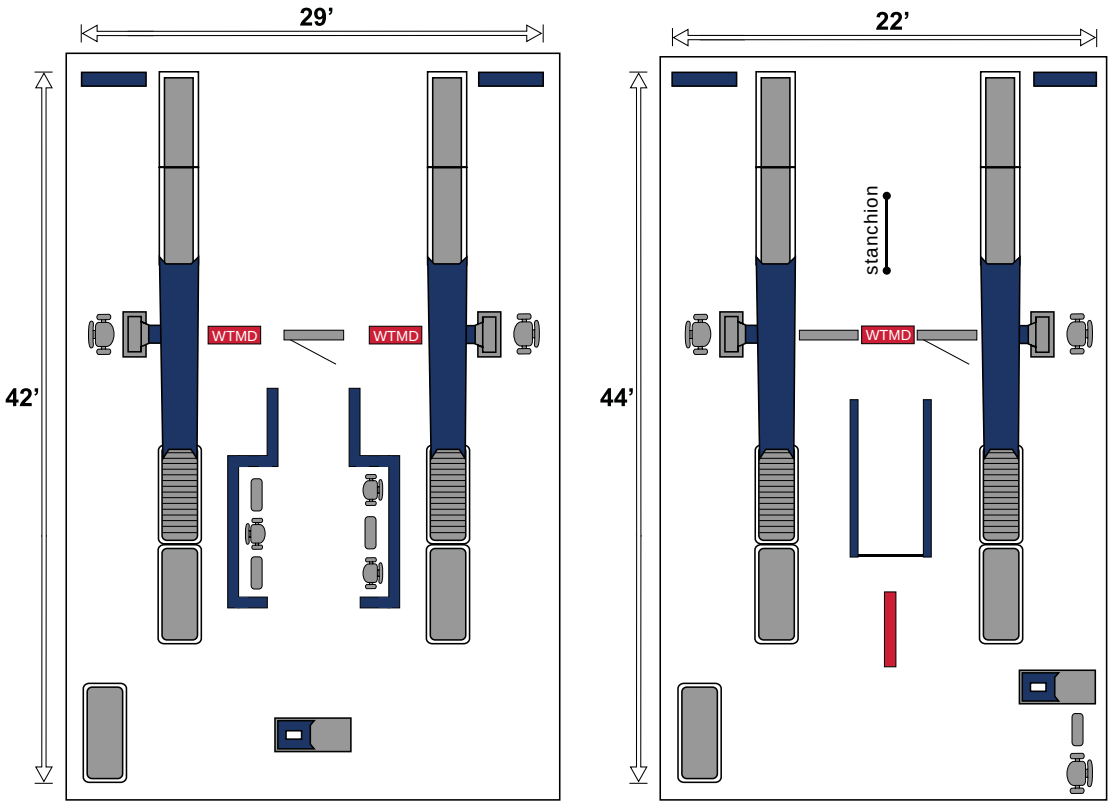


Figure III-E-13 - Typical 2-Lane SSCP Designs

Features of the Standard 2 to 2 Design with Wanding Station: (Refer to *Figure III-E-13* above)

This is a very common early TSA design. Each lane has one WTMD supported by one x-ray unit. The wanding station is centered directly (4') from each WTMD. The wanding station is used as a containment and secondary screening area. Each lane includes two divesting tables and one composure table; however the quantity or overall length of tables may increase depending on the type of passenger at the peak time of day. Passengers divest on the non-sterile (public) side, and the time they spend "composing" is significantly higher than the time spent waiting for items to go through the x-ray machine. Special consideration is needed to ensure the depth of checkpoints can support divest and composure tables.

The advantages of this design include open spacing that allows for easy flow. Selectees or WTMD alarmed passengers can easily be diverted into the wanding station where they can undergo secondary screening immediately. The wanding station is located such that the passenger can easily maintain eye contact with his/her baggage. The main disadvantage of this design is the fact that it requires the greatest amount of floor space.

Features of the Standard 2 to 1 Design with Holding Station: (Refer to *Figure III-E-13* on page 107)

This is a newer TSA design that is becoming more prevalent. This configuration consists of one WTMD centered between two x-ray units. The holding station is centered directly (4') from the WTMD. The holding station is used as a containment area until a screener becomes available to conduct secondary screening. This screener escorts the passenger from the holding station to an area designated for secondary screening.

Consideration is needed to ensure that the depth of the checkpoint supports divest and composure tables, as well as the area necessary to conduct secondary screening. It is important that a stanchion be placed 3 feet in front of the WTMD that separates passengers in each lane. Without this stanchion, the two lines tend to intermingle and become inefficient and insecure. Separating the two lanes is advantageous because when one lane's throughput stops, due to passengers recomposing or other issues, the WTMD screener can still permit passengers from the unaffected lane to flow through the WTMD.

The primary advantage of this design is the fact that overall width is only 22 feet. This design also allows great flexibility for screeners to work among different checkpoint lanes.

The disadvantages of this design are the slightly increased depth needed for the secondary screening area.

Features of the Standard 2 to 2 Design with Wanding Station and ETP:

This is the same design concept as the Standard 2 to 2 Design with Wanding Station (*Figure III-E-13* on page 107), incorporating provisions for an ETP.

Many options exist for placement of the ETP, both pre-WTMD and post-WTMD.

Features of the Standard 2 to 2 Design with Holding Station and ETP:

This is the same design concept as the Standard 2 to 2 Design with Holding Station (*Figure III-E-13* on page 107), incorporating provisions for an ETP.

The principal disadvantage of this design is the limited range of options for ETP placement.

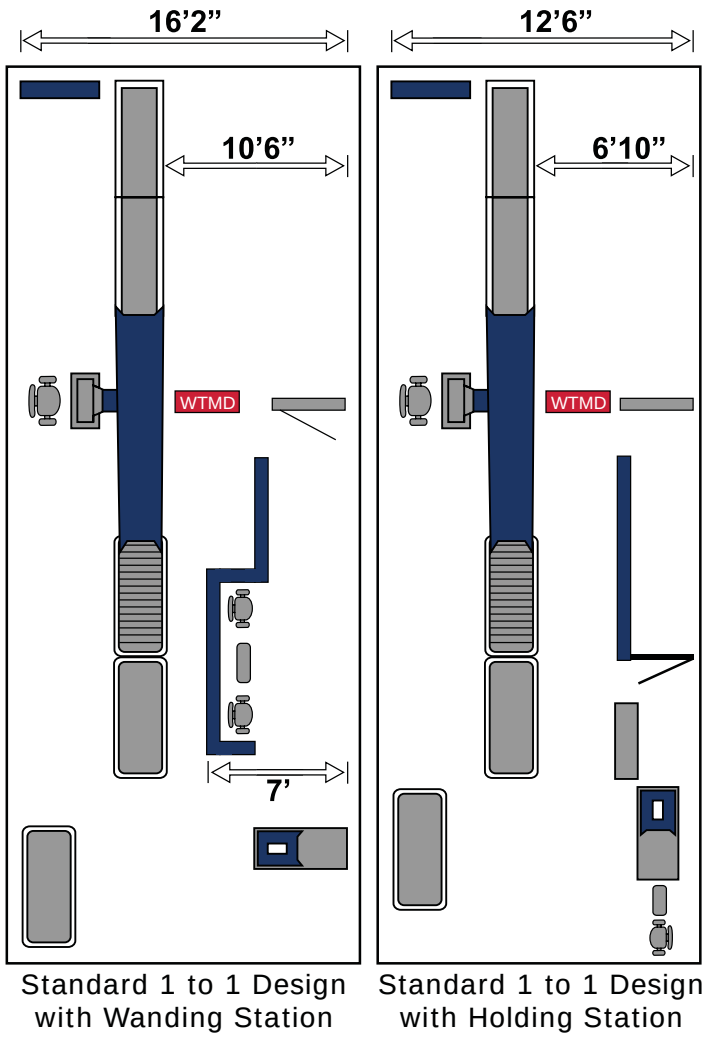


Figure III-E-14 - Typical 1-Lane SSCP Designs

Features of the Standard 1 to 1 Lane Design with Wanding Station: (Refer to *Figure III-E-14* above)

This is a very common early TSA design for one lane. A wanding station is created by placing glass partitions parallel to an existing airport wall. Two or three positions for secondary screening are located in the wanding station.

An advantage of this design is the secondary screening passenger can easily be diverted into the wanding station where they can undergo screening immediately.

A disadvantage of this design is the small amount of space available for additional technology to be added.

Features of the Standard 1 to 1 lane Design with Holding Station: (Refer to *Figure III-E-14* above)

This design is common in space-constrained areas or where a lane is added on either end of a checkpoint. The design consists of one WTMD and one x-ray unit. The holding station is most often created by a glass partition placed parallel to an existing airport wall. This design includes two divest tables and one composure table.

The advantage of this scheme is the small amount of floor space needed for the width of the lane.

A disadvantage of this design is the small amount of space available for additional technology to be added.

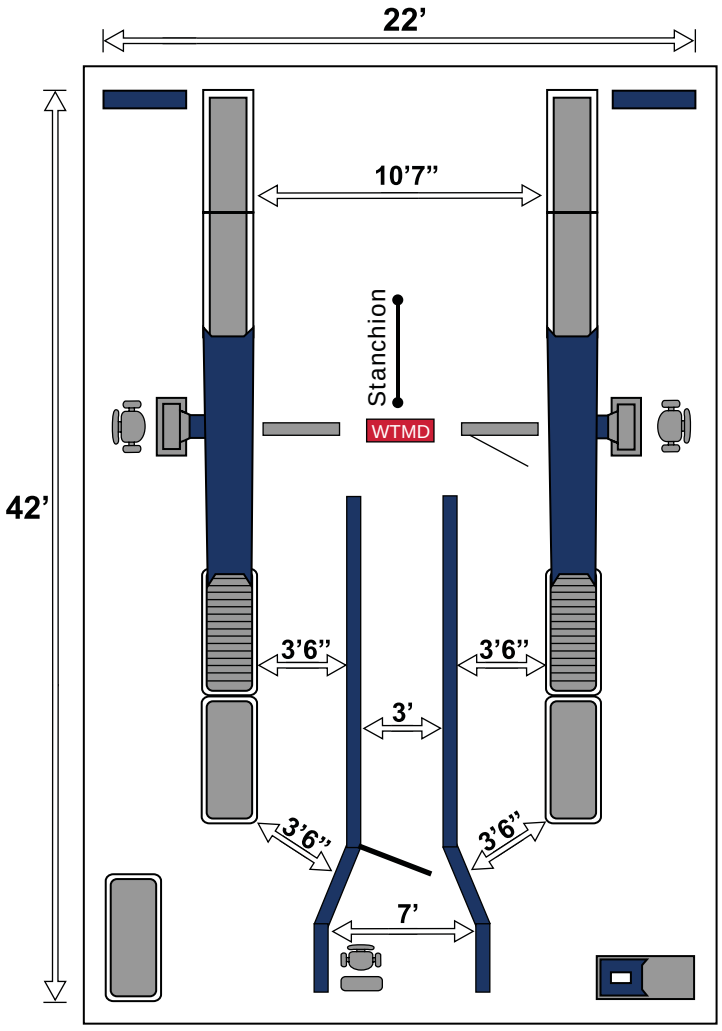


Figure III-E-15 - Typical 2-Lane Long Neck SSCP Design

Features of the 2 to 1 Design with Long Neck Wanding Station: (Refer to *Figure III-E-15* above)

This is the same configuration as a 2 to 1 Design with Wanding Station (*Figure III-E-13* on page 107); however there is an elongated neck, normally 9 to 12 feet long, on the front end of the wanding station. This neck is used to contain selectees and WTMD alarm passengers for secondary screening. The end of the neck is blocked by a door so the passenger cannot enter the wanding station until a screener is available.

Advantages of this design include the ability to queue passengers in the neck so that throughput of non-alarming passengers is not affected. The principal disadvantage of this design is the expense of the additional glass required for the elongated neck.

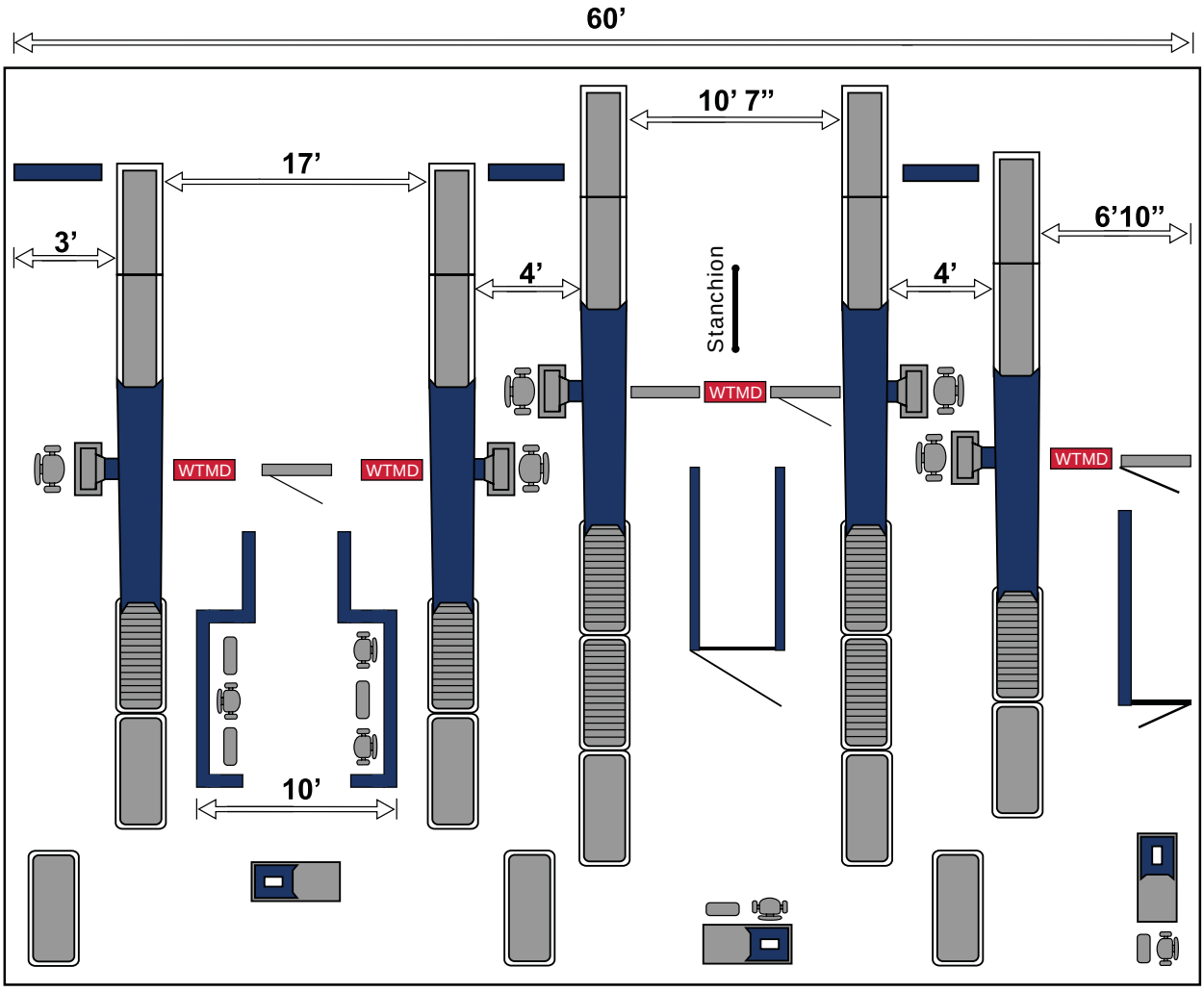


Figure III-E-16 - Typical 5-Lane SSCP Design

Features of the 5 lane Checkpoint with Different Configurations Combined: (Refer to *Figure III-E-16* above)

This layout illustrates the space savings from the combination of different lane configurations.

h. SSCP Spacing Requirements

The following chart is included as a reference to indicate the minimum clearance dimensions required for each piece of equipment.

Table III-E-6 - Typical SSCP Spacing Requirements

Approximate Dimension	Description
3′	Min. Distance From X-Ray Hood to Wall
5′	Min. side-to-side spacing between adjacent X-Ray roller tables
12″	Clearance between WTMD/EMD and X-Ray, barriers/ADA Gate, Walls, columns, and all other equipment. Barriers should be installed to close gaps greater than 15″. Barriers of non-metallic materials should be used as they have no effect on the operation of the EMD.
3′ 6″	Distance between X-Ray roller table and Glass Wanding Station.
4′	Distance between WTMD/EMD and start of Wanding Station Neck.
4′	Distance between WTMD/EMD and Holding Station.
7′	Interior width of standard two lane Wanding Station.
3′	Interior width of Holding Station.
8′	Min. length of single lane (one sided) Wanding Station.
4′	Min. Length of Wanding Station Neck.
8′	Min. length of Holding Station.
12′	Approximate length of Wanding Station screening area.
3′	Min. opening for ADA gate. Total outside width of ADA gate with posts is 3′ 11″.
6′ 6″	Distance from WTMD to ETP.
1′ 6″	Min. clearance for ETP side panels for service and maintenance functions.
6″	Min. clearance on-top of ETP for air flow.

i. SSCP Project Funding

The Airport, TSA and the planner/designer of a SSCP should coordinate and determine responsibility for costs involved with design and construction. This coordination is a necessary function for determination of funding responsibility reference components of the SSCP.

j. Designing for the Future

There are numerous government and commercial entities continually involved in the development of new technologies and concepts to enhance security. Some are still in the primary stages of conceptual development, or are enhanced derivatives of earlier technologies that are being revised after field-testing.

Airport security technology is a dynamic and rapidly changing field. No matter how carefully an airport is designed to take maximum advantage of the current technology, designs must be sufficiently flexible to meet changing needs and hardware. Machines may get smaller or faster, or both, requiring the entire

airport security managerial infrastructure to make important and often expensive decisions for modifications, which the designer must then accommodate. The designer's task will be easier if the original design has anticipated the need for change.

Evolving technology that may be considered by planners and designers today includes:

1) Bulk Explosives Detectors

   Bulk detection refers to technologies that determine the presence of explosives based on unique characteristics of a physical mass. Examples of bulk detection technologies for checkpoint screening include EDS and nuclear quadropole resonance (NQR), as well as other new technologies under development. Similar to existing screening concepts, these explosives detection devices will require areas for loading bags onto conveyor, areas for equipment, areas for the operator, areas for conveyor exiting the equipment and areas for secondary inspection which may involve reuniting the person with the item being searched.

2) Multi-detection Tunnel

   A future trend may be the integration of visual type searching of bags with explosives detection and metal detection devices into a single unified configuration. Some designers envision a short hallway or tunnel through which a person would walk, undergoing several types of search and detection in series. For example, part of the hall could be a metal detector, and another could be the trace detection system. The results of the scan tests could be monitored in a remote room. Simultaneously, the person's bags could run along a conveyor parallel to this hall, being scanned with EDS technology.

   A benefit of this hallway approach could be a perception of low intrusion on the passenger experience. A potential shortcoming could be confining designs with poor lighting creating an unpleasant experience. A challenge to this design is the inherent tendency of an enclosed hallway to prevent a visual connection between the person and the bags that are on a separate track. Fully or partially glazed walls could reduce this problem.

   At some point technology may be developed to enable a person to walk through the SSCP without being separated from their personal belongings and bags. In the United States, in some Customs locations, a person may choose to be subjected to a low-level EDS body search in lieu of a hand-search. In the current technology, the image of the body is blurred, while metal objects clearly show as hard images. This technology can also be used to identify concealed drugs on the body. This technology is not being used in SSCPs yet due to concerns about privacy and civil liberties. However, products are being developed to address these concerns. This technology may have applications in future SSCP designs, either as stand-alone units, or as part of the multi-detection hallway design.

3) Remote Screening / Monitoring Room

   Portions of the screening process can be automated by use of a remote room or area where security personnel can assess EDS and CCTV images and monitor SSCPs. Remote screening rooms are connected via data and communications connections to one or multiple SSCPs and may result in benefits such as reduced manpower, less operator distraction, and better capability to share screening personnel between multiple SSCPs during peak periods.

4) Automated Breach Detectors

   Some automated breach detectors already exist in airport applications; they use various technologies such as Doppler wave, infrared and others to allow passage in the appropriate direction while alarming if there is movement through the zone toward the sterile area.

5) Limited Application Explosives Trace Detectors

   Variations of ETDs are being developed that are designed specifically to screen tickets, boarding cards, documents, or other items handled by passengers.

Section III-E-1 - Security Screening Checkpoints (SSCP) Checklist:

☐ **Passenger SSCP issues**

- General issues
- Regulations & Guidelines – 49 CFRs 1542, 1544, 1546
- Essentials
- TSA, Airport and airline personnel should be consulted
- Planning Considerations
  - Level and type of risk
  - Airport operational type
  - Location of SSCP
- Elements of the SSCP
  - **A** - Prescreening preparation instruction zone
  - **B** - Queuing Space
  - **C** - Walk through metal detector (WTMD)
  - **D** - Non-metallic barriers
  - **E** - Non-metallic ADA Gate/Access
  - **F** - Carry-on baggage X-ray machine
  - **G** - Divest & Composure Tables
  - **H** - SSCP adjacent walls / barriers
  - **I** - Holding Stations
  - **J** - Wanding Stations
  - **K** - ETD machines
  - **L** - Egress Seating Area
  - ETP
  - Supplemental X-Ray
  - LEO Station
  - Supervisor Station
  - Private Search Area
  - CCTV Coverage
  - Data Connections/Cabinet
  - SSCP Lighting
  - Wireless Access Point
  - Exit Travel Lane
  - Exit Lane Station
  - Exit Lane CCTV
  - Integrated Exit Lane Systems
- SSCP Operational Efficiency
  - Designing for the Process
  - Length of Response Corridor
  - Architectural Design to Support Intuitive Processes
  - SSCP Signage
  - Space for TSA Staff
- SSCP Layout Standards
- SSCP Spacing Requirements
- SSCP Project Funding
- Designing for the Future
  - Bulk Explosives Detectors
  - Multi-detection tunnel
  - Remote Screening/monitoring room

2. Baggage Screening

a. Background

To meet the requirement for 100 percent checked baggage screening established in the November 2001 *ATSA*, the TSA approved the utilization of a variety of screening solutions. Many of these solutions were intended to be temporary since permanent in-line solutions require two to three years to complete from design initiation to system installation. Unfortunately, a good portion of the implementations were suboptimal by both operating cost and airport/airline impact metrics. However, this was necessary given the ATSA December 31, 2002 deadline (later extended by one full year) for 100 percent checked baggage screening.

Due to initial program schedule and space constraints at many airports, about 1,200 EDS machines were installed, primarily at CAT X and CAT 1 airports. Where EDS equipment was deployed, the machines were usually installed in airport lobbies. These initial deployments, considered standalone, were not integrated with the baggage handling systems which added to the already congested lobby facilities and processing times. To mitigate this impact and improve security, TSA has engaged with its stakeholders to improve the overall design of the checked baggage screening system.

The information contained within this section provides varying approaches that address the goals and objectives as stated above.

Remember, the formula for success is open communication and regular interface with all stakeholders throughout the entire design and implementation process.

b. Applicable Regulations

1) Regulatory Requirement

The *ATSA* signed into law on November 19th 2001 (Public Law 107-71, Section 110, Screening) mandates that the TSA shall screen all passengers and property prior to aircraft boarding and loading.

2) TSA Protocols

In general, the screening process using screening technologies may take place with stand-alone machines that are operated manually or via an integrated operation wherein the machines are incorporated in-line in the baggage system.

c. Protocols and Concept of Operations

Every terminal at every airport is unique. As such, many baggage screening system types need to be considered to find the optimal solution for each unique layout. Deployments are typically based on passenger demand at peak hours of operation. The effective throughput rate, not the machine scan rate, should be used in determining the number of certified machines (EDS/ETD) to install in a particular airport configuration (stakeholder coordination is mandatory to obtain required data).

The following data groups screening systems into five categories that range from high automation and low labor intensiveness (e.g., high-speed in-line) to low automation and high labor intensiveness (e.g., stand-alone EDS and ETD systems). The sixth category addresses emerging high-speed technology. Within each category, there can be one or more equipment models that contain similar throughputs, false alarm (FA) rates, and life-cycle costs. These categories of system types and protocols provide ranges for throughput and FAs. These ranges provide the designer with only an overview, and are not intended to address any one specific airport. To determine specific local needs, stakeholder involvement is critical. Further, specific airport needs will also help determine the appropriate screening approach.

1) Checked Baggage Screening Options

   a) Category 1: Fully Integrated In-Line Systems

   This category (refer to *Figure III-E-17* below) is the current state-of-the-art. These systems have multiplexed EDS technology, complex baggage handling system(s), control room(s) (central or local), On-Screen Resolution (OSR) capability, recirculation system(s), multiple baggage inputs, and checked baggage resolution room(s). These system capabilities are discussed in greater detail in this document. (Refer to *Table III-E-8* on page 122 and *Table III-E-9* on page 123 for further information.)

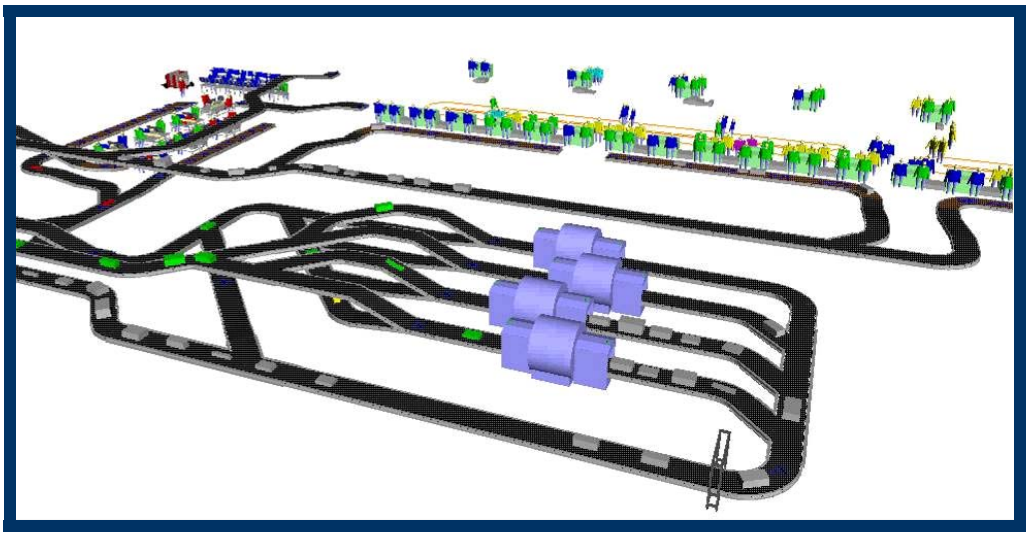


Figure III-E-17 - Category 1: Fully Integrated In-Line System

b) Category 2: In-Line Systems

A mini in-line system (refer to *Figure III-E-18* below) would typically employ a simpler conveyor design and require a smaller footprint. These systems can be located closer to airline ticket counters, makeup devices, or both, which can help reduce travel time and the likelihood of improper baggage sorting. Due to the decentralized nature of these systems, staff and equipment needs will generally be lower than centralized systems given the variable load requirements. (Refer to *Table III-E-8* on page 122 and *Table III-E-9* on page 123 for further information.)

Note: *Depending on configuration multiplexing may be a viable consideration*

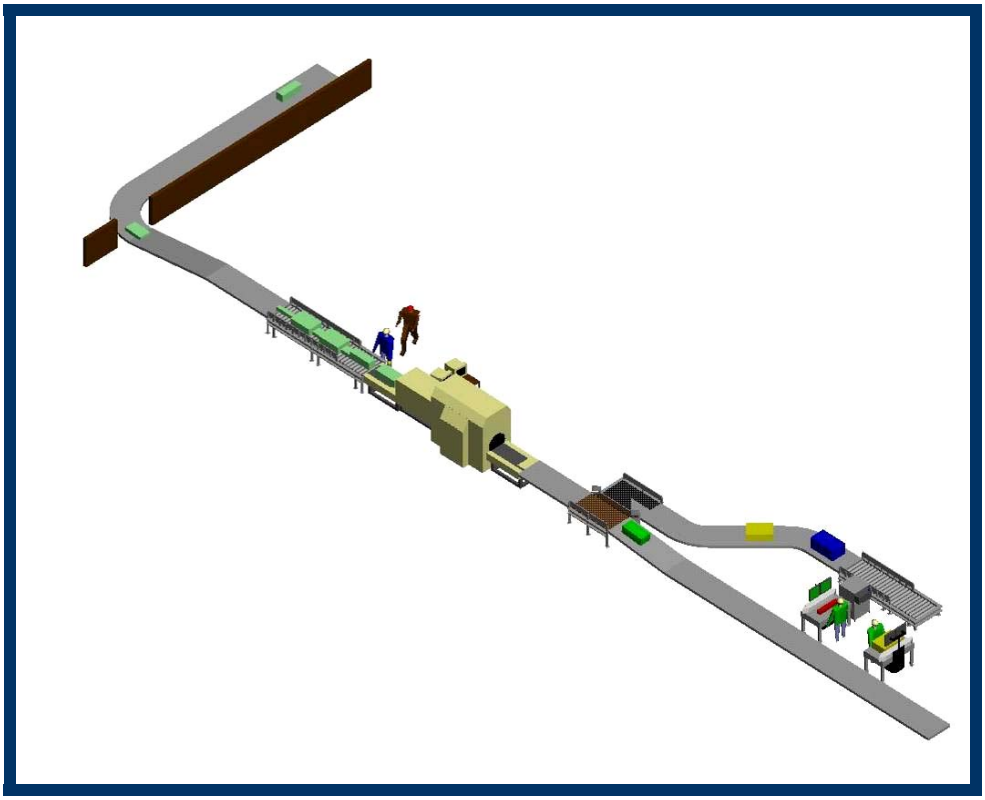


Figure III-E-18 - Category 2: In-Line System

c) Category 3: In-Line or Ticket Counter Mounted Systems

For facilities where architectural conditions exist that may render other systems cost prohibitive, a solution based on a compact, but low throughput machine placed at or near ticket counters may be the most viable economical option (refer to *Figure III-E-19* below). Their small size and low weight allow for design flexibility and a variety of possible system solutions. These types of systems also appear well suited for curbside deployment, for use with self-ticketing e-kiosk clusters, or low volume international recheck facilities (refer to *Figure III-E-20* below). They offer the lowest capital cost of any in-line system on a per machine basis, but are the least efficient in terms of throughput. (Refer to *Table III-E-8* on page 122 and *Table III-E-9* on page 123 for further information.)

Note: *Depending on configuration multiplexing may be a viable consideration.*

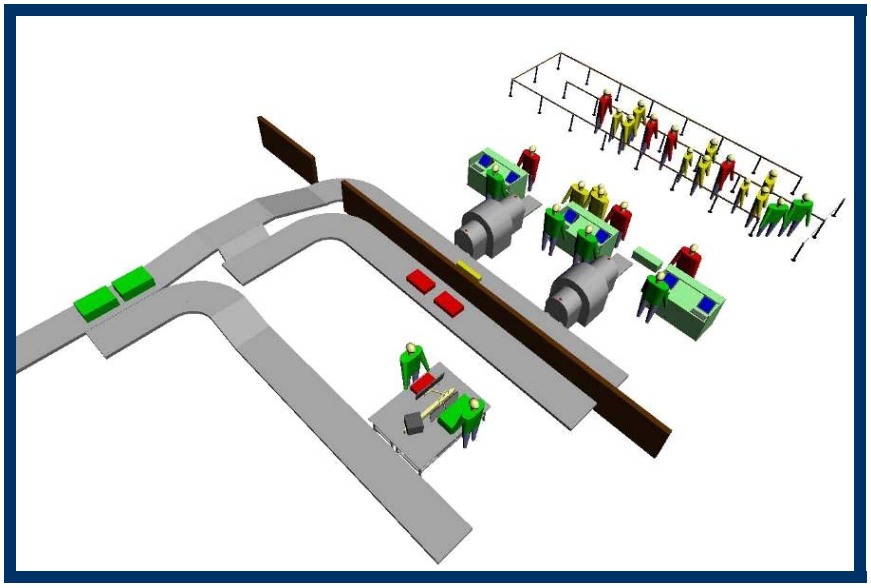


Figure III-E-19 - Category 3: In-Line or Ticket Counter Mounted System

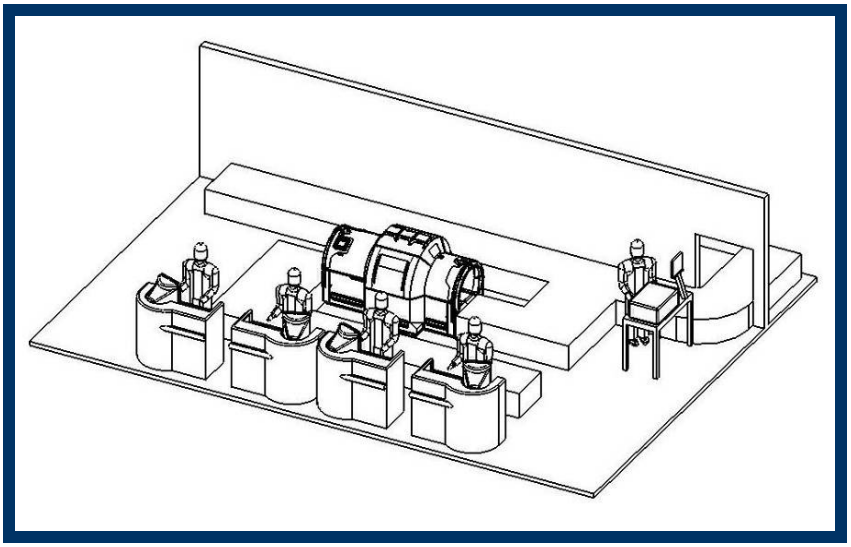


Figure III-E-20 - Category 3: Simple In-Line Ticket Counter System

d) Category 4: Stand-Alone EDS

For many smaller airports or small operations regardless of airport size, 100 percent EDS screening using stand-alone EDS (refer to *Figure III-E-21* below) in lobbies, baggage makeup areas, or other appropriate locations may be the most viable cost-effective option. These systems would operate in a similar manner to lobby screening nodes installed today at many CAT X and CAT I airports. However, sufficient equipment would be provided to ensure 100 percent EDS screening of baggage rather than current hybrid screening systems that use EDS as a primary screening method with overflow demand handled by co-located ETD equipment. (Refer to *Table III-E-8* on page 122 and *Table III-E-9* on page 123 for further information.)

Note: *Depending on configuration multiplexing may be a viable consideration*

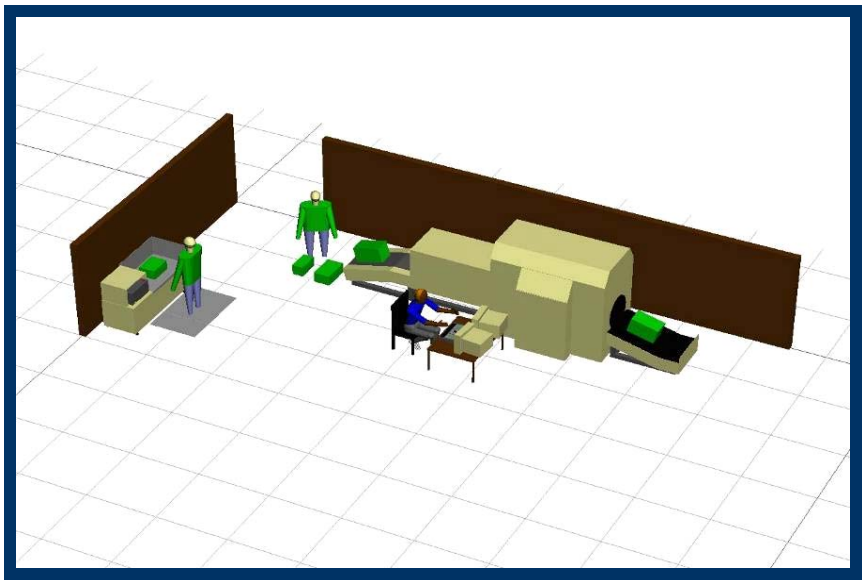


Figure III-E-21 - Category 4: Stand-Alone EDS

e) Category 5: Stand-Alone ETD Systems

As the most labor-intensive category, the final system type considered is 100 percent screening using stand-alone ETD (refer to *Figure III-E-22* below) in lobbies, baggage makeup areas, or other appropriate locations. Baggage should be screened using an approved protocol currently in place (contact local Federal Security Director [FSD] for specifics). These systems are appropriate for small operations and at small airports, due to the low throughput and staff-intensive nature of the process. For many of these locations, it may be possible to apply a more stringent protocol with little or no additional staffing or equipment requirements, but potential throughput impact may occur. (Refer to *Table III-E-7* on page 121 for further information.)

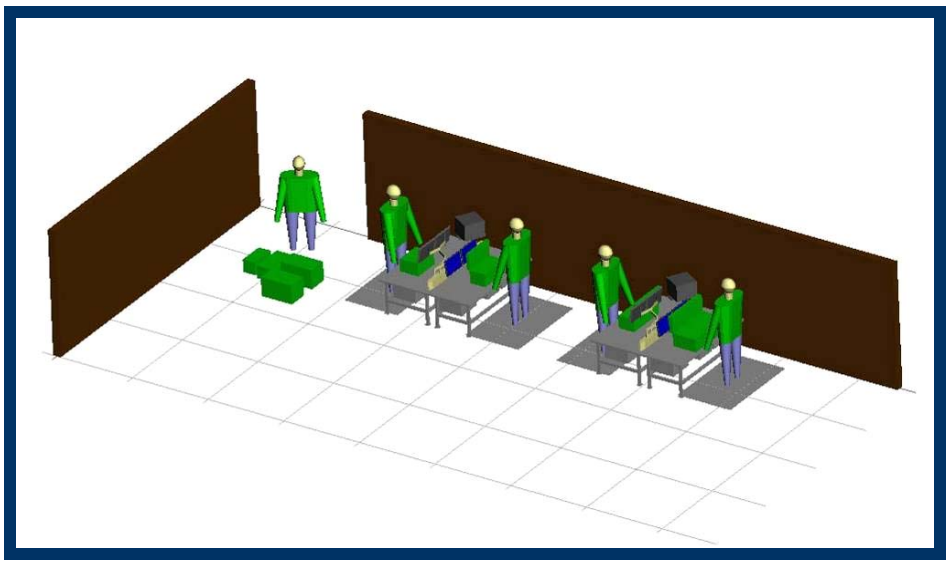


Figure III-E-22 - Category 5: Stand-Alone ETD System

f) Category 6: Emerging System Technology - High-Speed Fully Integrated In-Line Systems

High-speed fully integrated in-line systems (refer to *Figure III-E-23* below) are being developed, and assume the eventual availability of EDS screening technology currently in development under a number of TSA Research and Development (R&D) projects. EDS machines in this category are being designed to achieve a throughput of 900+ bph with an improved false FA. These high-speed EDS machines will be integrated into a sophisticated in-line conveyor infrastructure, providing sufficient queuing capacity (queuing capacity is critical) and OSR circulation time while maintaining high throughput and accurate bag tracking.

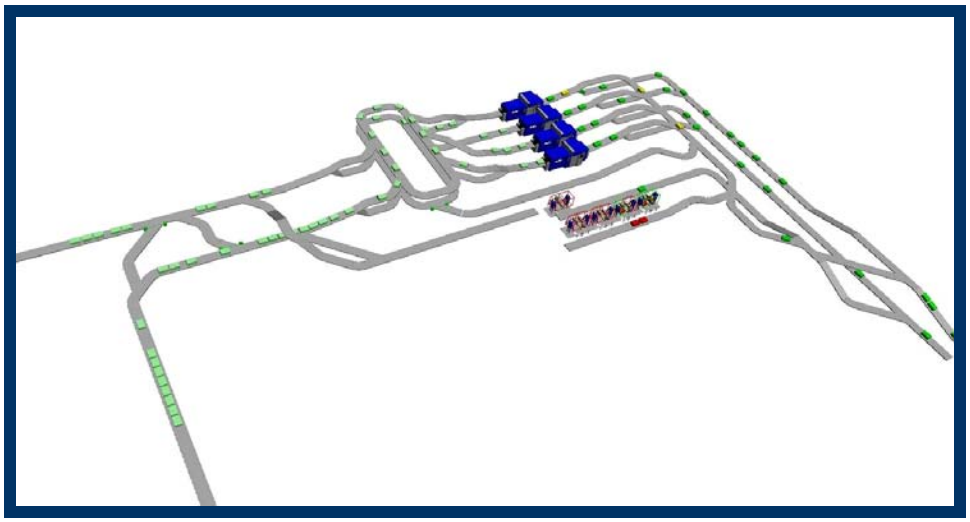


Figure III-E-23 - Category 6: Emerging System Technology

2) ETD and EDS Key Performance Characteristics

Table III-E-7 below, *Table III-E-8* on page 122, and *Table III-E-9* on page 123 are key performance characteristics tables of currently certified ETD and EDS as of the publication date of this document.

Contact the FSD to obtain the official and current TSA list of certified ETD and EDS to include a specific model's certified performance parameters.

Table III-E-7 - ETD Key Specification Characteristics

Notes: Coordination is required with FSD and all other appropriate stakeholders to obtain equipment requirements (type, number of units, etc.).
The information contained in this table was obtained directly from Vendor specification data. It is recommended that the vendor of choice be contacted for up to date information.

Manufacturer	Model	Width	Depth	Height	Power (110vac)
Smith's	Ionscan 400B	15.5″	13.5″	13″	6 amps
GE Ion Track	Itemiser II	18.9″	19.8″	16.3″	2 amps
Thermo Electron	EGIS II	28.5″	29″	18.5″	20 amps

Table III-E-8 - EDS Key Specification and Performance Characteristics

Notes: False Alarm rates are typically between 10 and 25 percent for domestic bag mix, and higher for international bag mix. The actual rate achieved in an inline system will depend on many factors associated with the design of the entire CBIS. Planners should reference TSA s CBIS performance in commissioning requirements to determine current minimum throughput rate design requirements for inline systems. Please contact local FSD for assistance.
The information contained in this table was obtained directly from Vendor specification data. It is recommended that the vendor of choice be contacted for up to date information. For new and emerging technologies see Category 6.

Model and Vendor	Throughput (bph)	Integration (Category)	Length	Width	Height	Weight (lbs)	Power (V)	Current (A)
GE/InVision CTX 2500	100-125	Cat. 2, 3, & 4	97″	75″	80″	7,350	480V 3-phase	13A
GE/InVision CTX 5500 DS (7.15.x upgrade)	200-250	Cat. 1, 2, 3, & 4	172″	75″	80″	9,350	480V 3-phase	13A
GE/InVision CTX 9000 DS	400-500	Cat. 1	187.4″	95″	87.5″	17,000	480V 3-phase	40A
L-3 eXaminer 6000 (Entry/exit specifications not included)	400-500	Cat. 1&2 (Cat. 4 capable, not preferred)	82″ (CT scanner only)	81″	86″	6,700 (CT scanner only)	208V	30A
Reveal CT-80	60-80	Categories 2, 3, & 4	95.5″	55.3″	58.3″	3,700	240V 1-phase	15A
AN 6400 (Entry/exit specifications not included)	400-500	Cat. 1&2 (Cat. 4 capable, not preferred)	86.5″ (CT scanner only)	81″	83.5″	6,700 (CT scanner only)	208V	40A

Table III-E-9 - EDS Key Baggage Specifications

Note: The information contained in this table was obtained directly from Vendor specification data. It is recommended that the vendor of choice be contacted for up to date information.

Model and Vendor	Bag Length	Bag Width	Bag Height	Bag Weight
GE/InVision CTX 2500	39.3″	25″	19″	110 lbs.
GE/InVision CTX 5500 DS (7.15.x upgrade)	39.3″	25″	19″	110 lbs.
GE/InVision CTX 9000 DS	51″	40.1″	23.6″	110 lbs.
L-3 eXaminer 6000	54″	32.5″	24″	300 lbs.
Reveal CT-80	47.2″	31.5″	25″	220 lbs.
AN 6400	62″	31.5″	24.8″	300 lbs.

3) Design Goals

a) Design Factors

Several factors will influence the performance of the design. The designer should take time to understand how the screening process will work, and the amount of time needed for each function. Only when the entire screening process is understood, can the system be properly designed. Some of the areas of importance are listed as follows:

i) Alarm rate of EDS equipment,

ii) Maximum input rate of Baggage Handling System (BHS) to EDS (can limit throughput if not sufficient),

iii) Throughput rate of EDS,

iv) EDS entrance tunnel aperture size

v) EDS reliability and availability,

vi) Expected clear rate of bags from OSR, if applicable,

vii) ETD clearance time,

viii) Number of ETD locations and associated screeners,

ix) Number, location, and capacity of baggage input points (e.g., CBP FIS recheck, ticketing, curbside, etc.),

x) Speed of conveyors,

xi) Screening location and screening process for oversized and out-of-gauge bags,

xii) BHS parts storage,

xiii) EDS parts storage,

xiv) BHS control room,

xv) Remote operator workstation to interface with the EDS equipment,

xvi) Central Monitoring Facility (CMF),

xvii) Multiplexer control (preferable within the CMF control room),

xviii) Checked Baggage Resolution Area (CBRA), and overflow room if required, and

xix) Ingress and egress for threat resolution and TCU.

In understanding the system operations, consideration should be given to the possible operational changes that could occur over the life of the system. For example, as of this writing OSR is an accepted process for clearing a portion of bags that alarm. However, if OSR were to be suspended as an allowable process, system requirements would change. It is recommended that flexibility be built into the facilities design, since it is likely that the equipment used for screening, as well as TSA protocols, will continue to evolve.

b) Schedule Issues

An important consideration in any master design plan is implementation of the project schedule. It is imperative that the project manager and designer closely coordinate with the FSD relative to equipment selection, and the specific lead time required for receipt of the selected system(s).

It is also imperative to understand the impact of the Site Acceptance Testing (SAT) process on the overall schedule. Again, this dictates close coordination with the FSD.

c) Fail-Safe Screening

In the case of EDS screening, a fail-safe system is defined as a system that maintains positive control of baggage throughout the entire screening process, and is designed with the criteria that the default bag path results in the safest path over other possible paths.

Fail-safe screening is usually applied to the decision or diversion point where alarmed bags are separated from cleared bags. This positive control of baggage precludes bags from bypassing the screening process, as well as the potential introduction of explosives or other dangerous materials into cleared baggage after screening. Fail-safe design considerations should include the following:

i) System equipment design that ensures default bag delivery from input to EDS and from EDS to CBRA,

ii) Modes of operation that support fail-safe delivery of all baggage to and from the EDS, ETD, or both,

iii) Modes of operation that support manual tracking, screening, and delivery of oversize baggage,

iv) Modes of operation that prevent the possible contamination of cleared baggage, and

v) Positive control of alarmed bags to prevent the inadvertent transfer of alarmed bags to the cleared line.

d) Maximizing Automation

The primary goals of automating the EDS process are to facilitate fail-safe baggage screening, increase throughput capacity, and reduce recurring operational costs. Automation of the screening process also provides the following benefits of efficiency in labor, space allocation, queuing, power, communication, and alarm resolution:

i) EDS multiplexing and networking to reduce the number of screeners and optimize airport operations,

ii) Increase in EDS productivity and reduced requirements for ETD,

iii) Automated handling of mis-sorted, lost, alarmed baggage, and mis-handled baggage,

iv) Improved standardization, and

v) Flexibility to accommodate advances in technology (e.g., Radio Frequency Identification ([RFID], Global Positioning System [GPS] tracking), and potential increase in screening throughput and capacity.

e) Baggage Handling

After acceptance by the airline from any location, on or off airport premises, bags need to remain sterile and secure. Areas must be provided that prevent access by unauthorized individuals. Securing an area is essential for preventing both pilferage and the introduction of items into baggage after they have cleared screening. Provision of separate, secure storage facilities should also be considered.

i) Minimizing Baggage Delivery Time from Check-In to Make-Up

In general, most airlines will not increase their flight closeout times or significantly increase staffing to accommodate the addition of EDS requirements. Factors that need to be considered to minimize effect of EDS on baggage delivery time include:

- Ticket counter die back process,
- EDS machine processing rates,
- Baggage handling system parameters set to regulate maximum allowable time of bags in system,
- System conveyors for cleared baggage,
- Load balancing of baggage handling and screening loads,
- Immediate separation of cleared from alarmed bags to expedite delivery of cleared bags to make-up area, and
- Baggage sortation scanning arrays should be located downstream of the EDS areas for optimum operations in inline systems.

ii) Diversion of Out-of-Gauge Bags

An out-of-gauge bag is a bag that can be introduced to the BHS, but due to the aperture size of the EDS tunnel will not physically fit into the entrance of the EDS machine (see Table 3). Bags that go through the dimensionalizer will be diverted to CBRA. Diverting bags before entering the EDS area reduces the frequency of jams caused by over-height and over-length conditions. BHS systems that generate bag ID, the out-of-gauge bags are differentiated from screened bags by the use of a specific bag ID.

iii) Oversized Bags

Oversized bags that are too large for the BHS will be routed to the CBRA, either by a dedicated oversized belt or manually delivered.

iv) Diversion of Alarmed Bags

The default conveyor path for all bags in the EDS area should ensure that in the event of a conveyor diverter failure all bags are routed to the CBRA. System design should not allow unscreened or alarmed bags to pass into the main sortation system or baggage make-up. Should this situation occur, alarms or other recovery methods must be implemented (see Section 3.3.10 for additional information).

The design criteria for the diversion of alarmed bags should support fail-safe operations. A clear chain of custody should be established for alarmed bags.

v) Handling of Selectee Bags

Airline passengers matching certain guidelines defined by the TSA are considered to be a selectee passenger. The TSA may or may not require special handling or processing of selectee bags. However, system designs should include the flexibility and capacity to add this feature (with minor modifications), if special handling is necessary to process these bags under more restrictive guidelines. The system, as a minimum, should be able to recognize a selectee bag status, and automatically route that bag to the CBRA.

vi) International Connecting Bags

Bags arriving from foreign countries must be screened before they can continue on U.S. flights.

International connecting baggage falls into two categories for clearance:

- Pre-Cleared Baggage: Bags arriving from international pre-cleared destinations (e.g., major Canadian cities, Bahamas) connecting to domestic destinations will require re-screening. These bags may be screened at a dedicated area on the ramp, or introduced into the BHS.
- Recheck Baggage (from international arriving flights): Recheck bags may be introduced at a recheck area just after the passenger clears FIS processing, or may be reintroduced at the ticket counters.

Peak-hour connecting bags can be estimated using the following data:

- Bags per passenger,
- Airline international arriving flight schedule appropriate for the chosen planning horizon (including arrival time and number of seats on aircraft),
- Load factor (total passengers on each flight, expressed as a percentage of total seats),
- Recheck factor (number of international to domestic connecting passengers, expressed as a percentage of total passengers), and
- Processing time distribution for FIS (for recheck baggage).

Note: Domestic connecting bags do not currently require any re-screening.

It is imperative that the FSD be involved throughout the design process.

f) Capacity Concepts

The design should consider sufficient system capacity without overbuilding. Optimal system design should address the following issues when developing operational performance criteria (this is not an inclusive list):

i) Clear definition and analysis of critical operational criteria

ii) Allowances for revisions with respect to passenger loads

iii) Forecasted baggage-to-passenger ratios, baggage size and weight, international rechecked bags, location of baggage check-in (e.g., curbside check-in, ticket counter check-in, remote check-in)

iv) Peak hour demand (number of originating flights, load factor, and passenger to checked bag ratio)

v) Existing and planned equipment throughput and reliability rates

vi) Balancing of baggage handling and screening loads

vii) Baggage handling system recirculation parameters for metering delivery of bags to EDS machines

The design should provide for adequate system capacity to avoid gridlock. Gridlock can occur when the actual baggage arrival rate exceeds the maximum designed system or subsystem capacity, and process rate. To minimize this potential, systems should be designed for flexibility that allows for a tempering to excessive peak flows, and the distribution of baggage to use EDS load balancing in low flow conditions.

Design considerations for mitigating excess system demand include:

- Baggage recirculation upstream of the EDS. Recirculation should only be considered for unscreened bags. Think of it as a baggage storage loop upstream of the EDS. Re-circulating bags downstream of the EDS quickly leads to unacceptable mixing of cleared, suspect, unknown, and unscreened bags.
- Adequate queuing conveyors feeding to, and discharging from EDS devices and CBRA,
- System redundancy in critical areas (including redundancy in controls),
- Back-up modes of operation in the event of conveyor or EDS equipment failure,
- Programmable options to provide flexibility in adapting to irregular airport operations, and
- Catastrophic bypass capabilities that should be designed into all systems to allow baggage to by-pass the EDS matrix, and arrive directly in the CBRA.

g) System Maintainability

Adequate space and right-of-ways in the EDS areas are needed to allow the following activities:

i) Access to EDS components for maintenance and replacement (refer to the EDS Vendors Installation Manual),

ii) Ready access to conveyor components and devices (e.g., motors, control devices) for clearing bag jams, equipment repairs, and resolving problems (adequate crossovers in the baggage sortation matrix areas),

iii) Code compliance for maintenance and operations egress, and

iv) Access by screeners to clear baggage jams, and conduct daily tests.

h) Ergonomics

The purpose of addressing ergonomics in this document is strictly to highlight to the designer the importance of this area in developing a BHS.

See the U.S. Department of Labor Occupational Safety & Health Administration (OSHA).

www.osha.gov/SLTC/ergonomics

www.osha.gov/SLTC/etools/baggagehandling/index.html

www.osha.gov/SLTC/etools/computerworkstations/components_monitors.html

i) On-Screen Resolution Facility (OSRF)

EDS images of suspect and alarmed bags are sent to the OSR Facility (OSRF) for review by TSA operators. There are two system configurations for this function:

i) A local OSRF control room is usually associated with a single cluster of EDS while a centralized OSRF control room monitors several EDS clusters.

ii) Centralized OSRF control rooms require less staffing, due to load sharing of screeners during off peak periods.

Typically, a centralized OSRF control room will require restrooms, a break room, supervisor offices, an Information Technology (IT) room, an uninterruptible power supply (UPS) room, and a mechanical room and storage space. The number of devices, EDS, OSRF monitoring stations, a computer interface station (CI), ETD work stations, and printers that can be networked together will vary depending on the EDS vendor and version of the networking software.

The number of OSRF screener positions needed should be determined based on the number of EDS machines in the design, the projected bag volume, the expected alarm rate, OSRF clear rate, and time needed to resolve an alarm. The design of the OSRF control room should be an open space with a centrally located supervisor position, with line of sight to all workstations. There should be direct access to either landside or airside, depending on how staff will arrive during shift changes.

j) Checked Baggage Resolution Area (CBRA)

The CBRA is the area to which EDS alarmed bags, oversized bags and selectee bags are sent for ETD screening. The basic layout provides for a delivery conveyor with bags to be screened, an inspection table with ETD equipment, bag status display, EDS control interface work station and an output conveyor for re-introducing cleared bags to the baggage sortation system. A conveyor line for re-introduction of unknown baggage back into the screening matrix is advisable.

The number of ETD screening positions and their configuration is determined by the throughput and alarm rate of the EDS matrix.

The key to the design of the area is to provide for the removal of suspect bags by providing an unobstructed path to and from the baggage search area sufficient in width and turning radii to allow for access of robotic vehicles. These vehicles are designed to access a typical 6 feet 8 inches tall by 36 inches wide doorway, and should provide 48 inches clear (44 inches minimum) for maneuvering in and around the suspect area.

As most robotic inspection vehicles provide control and video via a fiber-optic umbilical, the path between the command and control vehicle, and the baggage search area should minimize the number of turns and elevation changes, and reduce or eliminate the potential snag points. While most robotic vehicles are capable of climbing stairs and ramps of up to 45 degrees, ramps with a slope of less than 30 degrees are preferred.

Further consideration needs to be given to the ingress and egress of TCU. For additional guidance, please contact the FSD.

i) Explosive Resistant Area: Some airports have added explosive resistant areas, and some have considered hardening the entire baggage inspection area for disposition of suspect bags. These facilities have generally proven prohibitively expensive, or operationally unsuccessful. Hardened facilities can generally be designed to fully contain the effects of relatively small explosive charge. This type of containment design will expedite a return to operations.

ii) Bag Re-Introduction Belt: The baggage inspection room should also have a convenient bag re-insertion conveyor back to the EDS screening area. This is to allow TSA screeners to re-introduce bags from the CBRA to the EDS screening area should a bag arrive without an image.

k) Suspect Bag Removal

Due to the serious nature of this subject matter, greater detail has been provided in this section. Please contact all stakeholders to insure that design build-out is predicated upon the accuracy of information relative to local equipment requirements, applicable policy, and Bomb squad capability.

Unlike the conduct of the baggage screening process, which is established by the TSA, the requirements for inspection and removal of suspect bags falls entirely on the local Law Enforcement Officer (LEO) Bomb squad. Due to the differences in philosophies of different agencies, it is important to include discussions with the local LEO Bomb squad so that their unique requirements can be factored in as early as possible in the design process. Depending on the familiarity of the local Bomb squad with the airport, airport staff may also need to educate the Bomb squad on the nuances of airport operations to avoid needlessly complex or expensive design solutions.

A location for parking the Bomb squad command and control vehicle (typically a van), and a TCU in proximity to the baggage search area is essential. An airside location is generally preferred. This parking location should permit access to any point in the CBRA within the limits of the 300 feet umbilical connecting the robotic vehicle to the command and control vehicle. Any doors or closures between the two should provide electric, self-opening doors to enable the robotic vehicle to have a free and unobstructed access along its path of travel.

While the means to provide for removal of a suspect bag to an explosive containment vessel for transport to a safe location should be provided, the local Bomb squad may elect to diffuse any Improvised Explosive Device (IED) in-place in the CBRA. Correspondingly, it is important that the design of and operation of the CBRA allow for only inspection, not storage of bags. This is to avoid both bag clutter interfering with access by the robotic or human inspection team, or to avoid confusion as to which bag among the many in the area is the actual suspect. Furthermore, this access needs to also consider bomb squad access to the baggage delivery conveyor, given the EDS screener may flag a suspect bag prior to its arrival in the baggage inspection room, and TSA hand inspection.

It should be remembered that once TSA screeners discover a suspicious object, they relinquish control to the Bomb squad, and are unlikely to further handle the suspicious bag that may be open. As a result, provisions for relocation of suspicious objects via conveyors or carts to a more secure location are unrealistic. Furthermore, within the operating protocol of many Bomb squads, once a suspicious item is identified, the CBRA itself, and a large perimeter around it is evacuated; thereby, impacting nearby public areas of the terminal regardless of the size of the threat or any proposed containment.

Note: Some airports have a conveyor line dedicated to carrying an IED out of the CBRA and terminal building. The catch is that a person must manually place the probable IED on this conveyor; so, such hardware may prove to be of little use.

l) Contingency Plans

There are a number of contingency plans that exist in an airport environment that, when executed, will have a direct impact on checked baggage operations. These plans include those of federal,

state, and local jurisdictions, and must be considered by the designer during the planning phase. The following list is an example of these plans.

i) Change in the HSAS threat condition

ii) Change to regional or local threat level

iii) Airport Operations Emergency Response Plan

iv) Local Standard Operating Procedures (SOP) for transportation security incidents

v) Airport Emergency/Incident Response Plan

vi) Airport Emergency/Incident Recovery Plan

vii) When an incident or change in security level occurs, the following are examples for design consideration:

viii) Temporary screening location for baggage

ix) Egress points during emergencies

x) Threat evacuation and associated impact on baggage screening

xi) Emergency-stop (push button) locations

xii) Natural disaster impact on screening space

To meet the needs for contingency planning, it is critical that close co-ordination occur between the airport authority, FSD, and all other federal, state, and local authorities.

m) Environmental Impact

The operational environment of an airport can vary significantly; therefore, the following factors should be considered:

i) Environmental Stress:
- Humidity
- Low pressure altitude
- Loose particle contamination
- Temperature

ii) Mechanical Stress:
- Shock
- Vibration
- Acoustic noise

iii) Electromagnetic Interference (EMI):
- Conducted susceptibility
- Radiated susceptibility
- Power fluctuations
- Conducted emissions
- Radiated emissions
- Electrostatic discharge

Most EDS units are equipped with self-contained air conditioning units that have specific ranges of operation. These units require a connection to a waste drain for condensation. Where ambient conditions exceed the manufacturer's recommendations, an environmental enclosure is recommended to keep the units operating at its maximum efficiency, and reduce maintenance cost from a complete systems approach. Consideration needs to be given to removing the EDS emitted heat from the internal air conditioning units.

Rooms will require environmental conditioning and access control. Consideration should be given to using raised flooring in both the server and control rooms for ease of cabling.

n) Communications

Communications capabilities for both data and voice for checked baggage EDS network(s) will require advanced design and planning. Established communications standards and policies should be followed when planning the integration of checked baggage screening systems and equipment to airport communication infrastructure. Design will include, but not be limited to, the following:

i) BHS
ii) EDS
iii) Baggage Viewing Systems (BVS)
iv) Search Work Station (SWS)
v) Security and fire systems
vi) Voice – telephone
vii) Security Identification Display Area (SIDA) access systems
viii) Radio Frequency Identification (RFID) tagging systems
ix) CBRA
x) Ticket counters
xi) Checkpoint locations

Refer to *Power, Communications, and Cabling Infrastructure* on page 180 for more information.

o) Engineering Issues

i) Maintenance Access and Removal

During the design phase, a rule of thumb is to add 48 inches (4 feet) to each side of the EDS machine footprint for maintenance access. This clearance is typically not required at the entrance and exit ends of the EDS machine. Additionally, some models currently require vertical clearances above the EDS machines. The actual, minimum footprint will vary in size and shape depending on the clearance required to open doors and slide out internal components. Check with the manufacturers for details pertinent to their models.

Sizing the openings into the areas where equipment will be located, or timing the placement of EDS machines before constructing enclosing structures, can eliminate cost and problems associated with getting the equipment into place. Consider including the ability to remove the equipment, replace or relocate equipment as needed, or during heightened threat conditions. Check manufacturer specifications for necessary turning radius and other clearances. Consideration during design should be given to providing for removal of a complete EDS machine from the system. Overhead crane rails or openings in the structure should be considered to avoid having to disassemble the operating system.

ii) Floor Loading

Floor loading for EDS security devices can be significant. Given the wide range of possible floor loading factors, all parties to the installation project should carefully review the devices that will be used initially, what might ultimately replace them, and what alternative locations within the structure may be available. It may be possible to distribute the weight using steel plates in retrofit projects where the existing structure will not support the load.

iii) Systems Integration and Operation

(a) Installation of Equipment / Phased Implementations

Because most screening installations will require integration of existing operations, it is imperative that the installations have provisions for complete checkout prior to introducing live traffic. The TSA document, Performance and Commissioning Master Plan, needs to be addressed during proposed implementations to assure compliance with TSA screening requirements (see FSD for document). This document is being updated routinely by the TSA as installations come on-line.

(b) Testing of Equipment

The Checked Baggage Inspection Systems Performance and Commissioning Requirements document addresses procedures for testing of equipment (see FSD for a copy of this document).

(c) On-Going Maintenance

The TSA provides for on-going maintenance of the EDS machines. During design and installation provisions for spare parts storage needs to be considered.

(d) Accountability for the BHS and EDS Integration

Performance of an installation is shared responsibility between the baggage system and the EDS personnel. Reporting systems must be developed and implemented to track system outages, durations, and requirements to restore systems to full operation. From design concept through commissioning and into operational mode, it is imperative that adequate and timely communication lines are established to ensure operating system integrity.

p) Americans with Disabilities Act (ADA)

The purpose of addressing ADA requirements in this document is strictly to highlight to the designer the importance of this area in developing a baggage screening system.

See the U.S. Department of Justice Americans with Disabilities Act (ADA) and the Americans with Disabilities Accessibility Guidelines (ADAAG) for requirements and guidance.

q) Closed Circuit Television (CCTV)

i) Surveillance

In addition, the local airport may require the installation of surveillance CCTV oversight of the baggage inspection areas to provide for defense against claims from passengers of inspected bags. Delivery and storage of CCTV images needs to be coordinated with local police and other agencies that may desire CCTV imagery within the terminal, and which may be able to share a common system.

ii) Operational

CCTV for the EDS machines can enhance operational and staffing efficiency by allowing some EDS faults to be cleared remotely, reducing the need to send a screener out into the BHS matrix to clear the fault.

d. Design Mitigation & Lessons Learned

In general, the areas of concern addressed in the following lessons learned are baggage tracking issues, the risk and impact of mixing cleared and non-cleared bags and the movement of checked bags in an orderly, controlled and timely fashion.

1) Avoid Steep Conveyor Slopes

a) Steep slopes lead to baggage rolling and sliding on the conveyor.

b) Baggage rolling and sliding on the conveyor results in tracking losses, bag jams, and bags doubling up.

c) Double bags inducted into the EDS often cause machine faults resulting in reduced throughput.

d) Double bags can lead to security violations if a suspect bag and a clear bag slide together and are cleared together.

e) Diverters and pushers are not effective in pushing double bags.

2) Manage Belt Speed Transitions to Avoid Tracking Loss

a) Large belt RPM transitions from belt to belt cause bag spacing problems which lead to tracking losses.

b) The most common bags that cause tracking issues are wheels-down bags, odd-shaped and small bags.

3) Photo Eyes Too Close to the Belt (Refer to *Figure III-E-24* below)
   a) Often miss the true leading and trailing edges of a bag.
   b) Bumps or curls in the conveyor belt can activate such photo eyes.
   c) These photo eyes are harder to adjust for straps and tags.
   d) Above all, they cause tracking losses and can cause bags to creep along the belt reducing bag spacing.
   e) Photo Eyes should be placed in a position capable of detecting the minimum height of an item the system may receive - typically 3 inches.

Figure III-E-24 - Photo Eyes Too Close to the Belt

4) Avoid Placing Photo Eyes Too Close to Conveyor Ends (Refer to *Figure III-E-25* below)
   a) Can result in baggage improperly moving to the next conveyor.
   b) The photo eye positioning in this example resulted in bags not stopping in time, transferring to the rollers, and falling on the floor.

Figure III-E-25 - Photo Eyes Too Close to Conveyor Ends

5) Avoid Static-Plough and Roller Diverters (Refer to *Figure III-E-26* below)
   a) Static-Plough and Roller Diverters have multiple jam points and will cause issues.
   b) Use of these diverter types, require frequent manual intervention.
   c) They are a safety hazard for operators, especially if jam detection is not provided as in this example.
   d) To address this issue, consider using high speed diverters.

Figure III-E-26 - Roller Diverters (Static Plough not shown)

6) Use Conveyor Brakes and Variable Frequency Drives (VFD) (Refer to *Figure III-E-27* below)
   a) The lack of brakes or Variable Frequency Drives (VFD) can lead to baggage queuing and spacing problems as un-braked conveyors coast to a halt resulting in tracking losses and machine faults.
   b) Where decision points are inserted into a system without brakes or VFD, security violations can occur when suspect bags coast onto the outbound belts and are carried away by the downstream conveyors.

Figure III-E-27 - Conveyor Brakes and Variable Frequency Drives (VFD is located under the belt)

7) Avoid Inaccurate Pusher Operation (Refer to *Figure III-E-28* below)
   a) Improperly timed pushers consistently rotate baggage causing jams on turns and at EDS entrances.
   b) If a jam occurs at a decision point, this can result in security violations when a push affects a bag for which it was not intended.

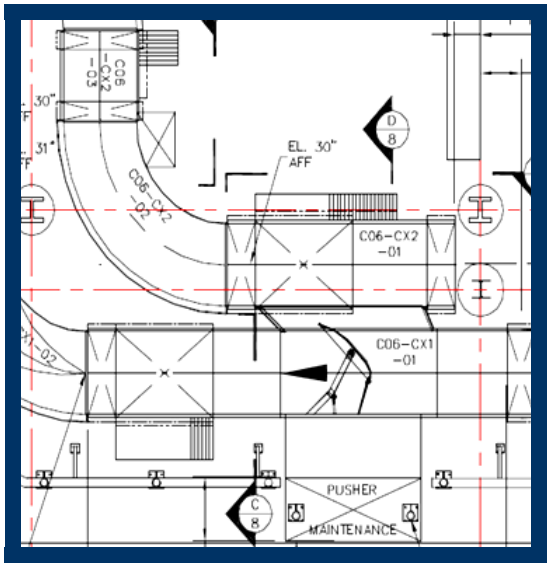


Figure III-E-28 - Inaccurate Pusher Operation

8) Avoid Improper Merging and Too Many Belt Merges (Refer to *Figure III-E-29* below)
   a) Systems that try to merge many lines together in a short distance end up increasing bag jam rates, increasing the number of incorrectly tracked bags, and reducing the overall throughput.
   b) This is frequently a factor in racetrack or looped systems where insufficient space is given to accommodate the required number of transitions to and from the loop.

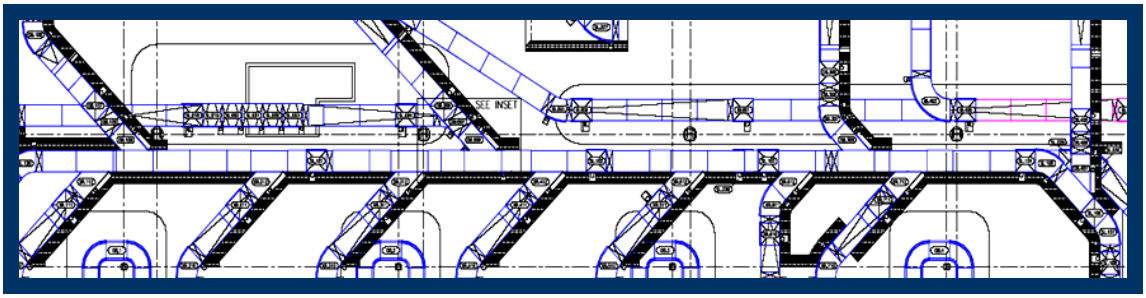


Figure III-E-29 - Too Many Belt Merges

9) Avoid 90-Degree Belt Merges (Refer to *Figure III-E-30* below)
   a) This type of design is more likely to cause jams and tracking losses than 45-degree merges.
   b) Proper placement of corner wheels or rollers reduces the risk of jams.
   c) In general, 90-degree merges have proved problematic when integrated into a Checked Baggage Inspection System.

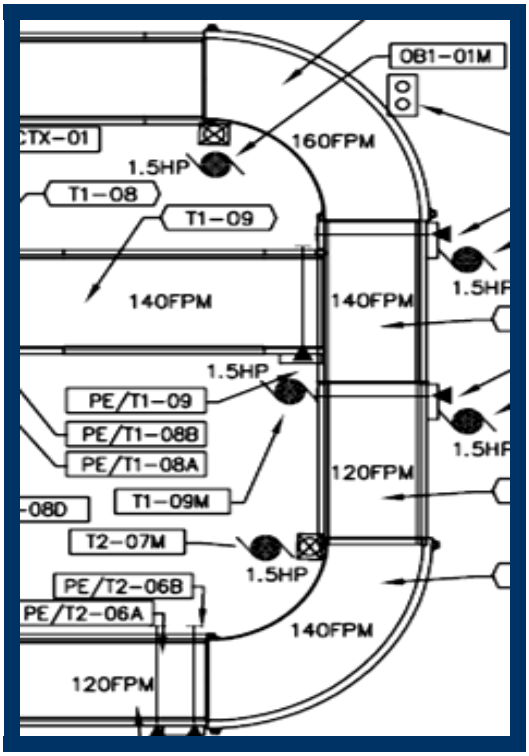


Figure III-E-30 - 90-Degree Belt Merge

10) Avoid In-Line Decision and Removal Points (Refer to *Figure III-E-31* below)
    a) Baggage tracking must be 100 percent accurate. Security breaches can occur when a suspect bag traverses the decision point and continues on to the outbound sortation system.
    b) This configuration reduces throughput. However, in other configurations it reduces space requirements, and is appropriate in certain situations.

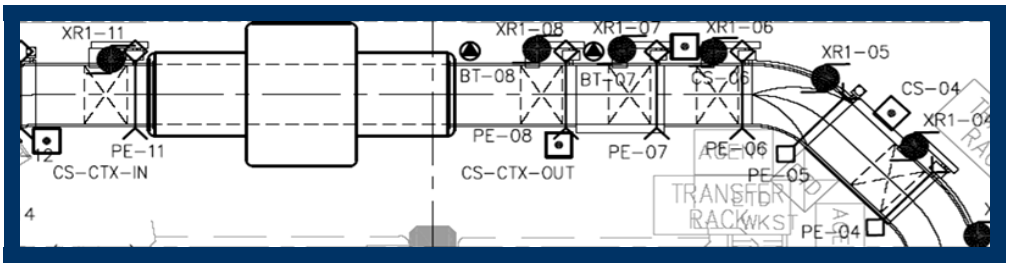


Figure III-E-31 - In-Line Decision Points

11) Avoid Directly Opposing Diverters (Refer to *Figure III-E-32* below)
    a) This configuration makes tracking difficult and reduces system throughput.
    b) Further, baggage can more easily jam and some baggage will traverse the center conveyor to the other line.
    c) In some configurations weighted vertical belts had to be hung across the diverter chutes so that bags would not soar over the intended receiving conveyor.

Figure III-E-32 - Directly Opposing Diverters

12) Lack of a Fail-Safe Decision Point (Refer to *Figure III-E-33* below)
   a) A system lacking a fail-safe configuration must correctly divert 100% of all non-cleared bags to the CBRA (see full discussion of fail safe system under Design Goal).
   b) The simplest way to be ensured that all non-cleared bags are never mixed with cleared bags is the integration of a fail safe configuration into the baggage system. The most commonly used fail safe device is a photo eye.

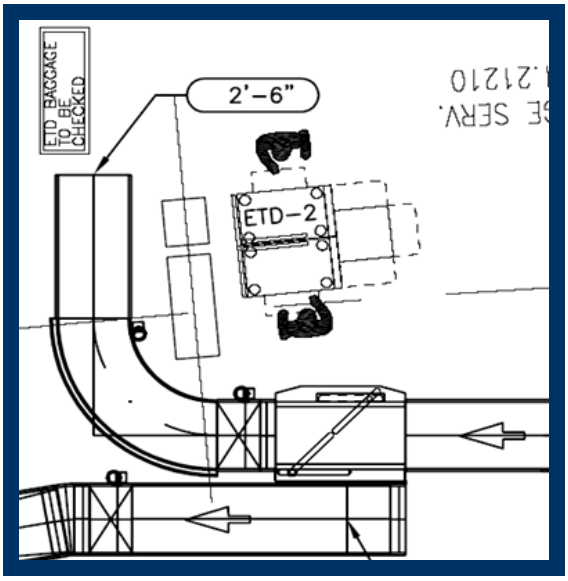


Figure III-E-33 - Conveyor Section without Decision Point Photo Eye

13) Avoid Reinsertion Points between EDS and Decision Point(s) (Refer to *Figure III-E-34* below)
   a) This configuration reduces throughput and complicates tracking.
   b) It complicates operations for TSA personnel.
   c) There is a security risk when bags are incorrectly inserted into the baggage system. A bag incorrectly placed back into the baggage system could result in a non-cleared bag entering the cleared line.

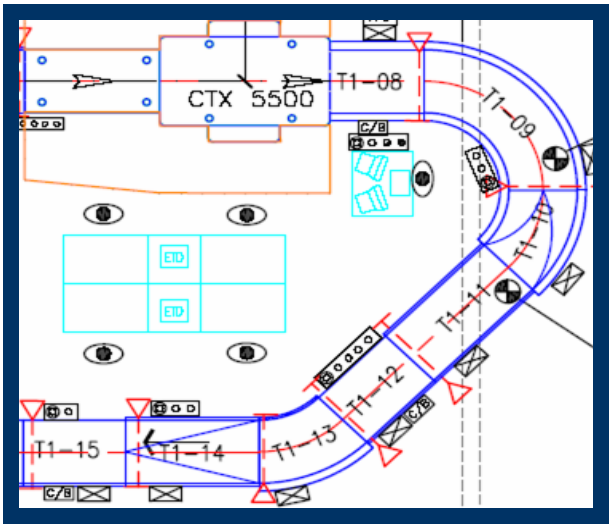


Figure III-E-34 - Avoid Reinsertion Points between EDS and Decision Point(s)

14) Avoid Bottlenecks (Refer to *Figure III-E-35* below)
   a) Merging two lines reduces system throughput and leads to frequent cascade stops.
   b) Consider using separate conveyors.

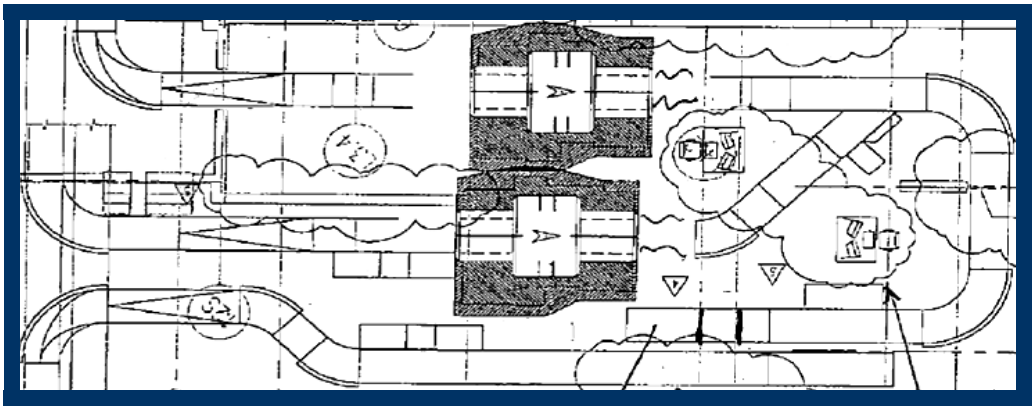


Figure III-E-35 - Bottlenecks Caused by Merge

15) Avoid Using Plexiglas Photo Eye Guards (Refer to *Figure III-E-36* below)
   a) Some photo eyes have been covered with clear Plexiglas sheets in an attempt to reduce bag jams.
   b) This results in a maintenance problem. The sheets get so scratched and scarred that they stop the photo eyes from working properly.

Figure III-E-36 - Plexiglas Photo Eye Guard

16) Avoid Short Reconciliation Lines (Refer to *Figure III-E-37* below)
    a) With a short reconciliation belt, a baggage flow increase would cause the system to stop and immediately cause dieback, possibly to outbound sortation.

Figure III-E-37 - Short Reconciliation Line on Left

17) Avoid Non-Powered Rollers (Refer to *Figure III-E-38* below)
    a) Non-powered rollers cause bag jams and tracking losses as bags slow, hang, and get caught on the rollers
    b) Frequent cleaning is also required as bag tags and other stickers get caught and adhere to the rollers.

Figure III-E-38 - Non-Powered Rollers

18) Avoid Power Turns at the EDS Exit (Refer to *Figure III-E-39* below)
    a) Bag jams are frequent. In this configuration longer length bags cause frequent jams.
    b) There have been at least two instances when the power turn and EDS tunnel ripped off the floor from the forces exerted in the jam.

Figure III-E-39 - EDS Exit Power Turn

19) Use Tubs When Appropriate (Refer to *Figure III-E-40* below)
    a) CBIS are not the simple non-tracked dump the bags to the carousels of yesterday. Bags must maintain positive tracking, and jams minimized.
    b) Vendors should work with airports to encourage tub use whenever bags are irregularly shaped, and straps or obtrusions are present.

Figure III-E-40 - Irregular Shaped Bags Causing Jams

20) Consider How Bag Orientation to the EDS will be Maintained (Refer to *Figure III-E-41* and *Figure III-E-42* below)
    a) Bags should be aligned, centered, and queued properly to achieve maximum throughput.
    b) Entrance bag jams affect the entire system as diebacks occur until the jam can be cleared.

Figure III-E-41 - Entrance Point Bag Orientation Jam

    c) Bump-outs shown in the foreground nudge tubs off the side wall. The iron arms just beyond the bump-outs center all the tubs.
    d) The tapered sidewall in front of the EDS cleanly lets the tub enter the EDS. Almost no bag jams occur with this system.
    e) EDS faults are reduced and image errors are almost eliminated.
    f) The drawback, of course, is that the airlines must all use one standard size tub.

Figure III-E-42 - Well-Designed EDS Entrance Conveyor

21) Use Caution with Draft Curtains (Refer to *Figure III-E-43* below)

a) Draft curtains should be cut to remain clear of nearest Photo eye (PE).

b) The weight of draft curtains can cause small and light bags to jam and to slip on the belt causing tracking losses whether the bag is in a tub or not.

c) Even heavy bags are affected by curtains. At one airport, draft curtains were used over a belt running at 240 bags per minute (bpm) where the bag window for tracking was plus or minus six inches. Almost 75 percent of bags were lost in tracking at the curtains.

d) The best solution is often to eliminate draft curtains in the tracking zone.

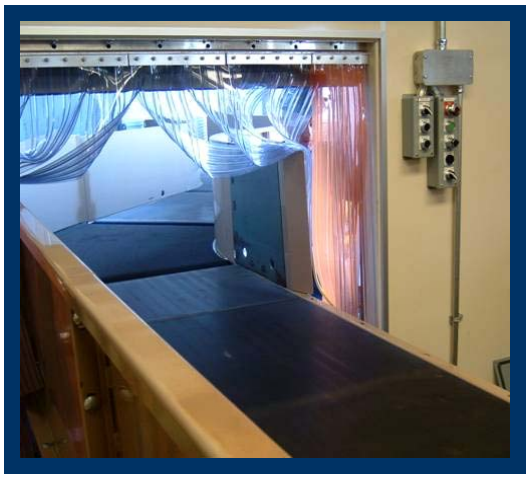


Figure III-E-43 - Eliminate Draft Curtains

22) Avoid Tracking without Real-Time Belt Speeds

a) Tracking baggage by measuring the speed of conveyors at installation, and hard coding that speed into the Programmable Logic Controller (PLC) will result in disaster

b) Belts stretch and slip over time, motors age and change speed, and gear boxes and pulleys wear. The conveyor speed measured today will not be the speed measured a week or a month from now. Airports have installed systems with no belt tachometers, no star wheels or encoders of any type. These airports have suffered tracking losses so frequently that reconciliation has been overloaded with clear bags, and worse, suspect bags have gone to the outbound sortation system. Use real time belt speeds in the design configuration of the PLC to avoid these problems.

23) Inefficient Baggage System

The most inefficient system mixes all bags of all statuses together. An example of this type of mixing is described below.

Baggage is introduced onto the far side of the loop. Baggage then circulates to the near side, where it is pushed at a 90 degree angle to the EDS, which spans the racetrack. All baggage is screened, and suspect, clear, and pending bags merge onto the far side of the racetrack with incoming unscreened luggage. Clear bags proceed to the side of the loop, and are pushed to outbound sortation. Suspect bags proceed back to the near side of the loop to CBRA. Once suspect bags are resolved, they return to the far side of the loop, mixing with clear, suspect, incoming, and pending bags before being diverted. Only three-quarter of the design throughput goal was achieved.

24) Efficient Baggage System

The most efficient system will quickly separate baggage based upon the screening status as described below:

Within a few queue conveyors of the EDS exit, Level 1 clear bags are diverted from the stream directly to outbound sortation. Remaining bags are allowed sufficient travel time to accomplish OSRF. The TSA recommends a 45 second minimum. Then, Level 2 clear bags are diverted to outbound sortation. At this point, lost in tracking, fault, and otherwise unknown bags are automatically routed back to the EDS entrance for re-screening. Finally, Level 2 suspect bags continue to CBRA.

The following are some examples of important issues that must be addressed:

a) Construction schedules must allow sufficient time for thorough test and inspection

b) BHS specifications should be developed with TSA criteria for CBIS performance, as defined in the TSA Master Test Plan

c) The commissioning process should be clear and open to all stakeholders, including Chief Technology Officer (CTO), local TSA, the airport authority, BHS contractors, and users of the system. Commissioning requirements should be made known to all parties before bidding takes place.

d) The selection of a CBIS contractor is critical. Airports with operational CBIS should be consulted and visited.

e) CBIS must be placed under configuration management and properly maintained. All belt speeds, belt textures, motor gear boxes, and PLC programming should remain consistent to ensure acceptable performance. Even small changes within the tracking zone can affect system performance. Complete Operation and Maintenance (O&M) manuals, with a maintenance schedule, as-built drawings, and current PLC program, should be required for all installs.

f) The maximum possible decision time should be provided before bags are recombined and sorted.

g) Immediately merging the outputs of EDS should be avoided as it has proven to be a complicated mixing of bags with different statuses. The best systems seen to date allow for one minute of travel and decision time, then divert clear bags, and then merge suspect lines for baggage transport to CBRA.

h) Bag ID and screening status displays should be a consideration for installation on all incoming reconciliation lines. Better information at CBRA results in higher system throughput. This capability will enhance CBRA results in higher system throughput.

i) Investment in PLC error logging and reporting or some other form of system diagnostic capability has proven valuable. It allows for monitoring of EDS and BHS performance, so that developing problems can be spotted early, directing preventative maintenance efforts.

e. Impact of Various Threat Levels on Screening Operations

Occasionally security threat levels will vary resulting in either an increase or reduction in security requirements. The impact of these changes may affect baggage screening time thus affecting flow. This dictates that the designer recognizes the need for overall design flexibility. For example:

1) Temporary space for baggage staging

2) CBRA search area(s)

3) Suspect bag retention and removal area

4) Reasonable vehicle access (e.g., Tug, pick-up, police vehicle)

f. Alternative Screening Options (Remote Screening)

Remote sites such as cruise ship terminals, airport parking areas and structures, hotels, train, ferry and bus terminals, car rental facilities, and other satellite ground transportation centers are all part of an inter-modal network that can connect travelers to an airport terminal. Many of these sites are either the points of origin,

or the link between modes of transit for those accessing the airport. In either case a trend for checking in baggage at such sites could be expected and attributed to both broadened security measures, and the improved levels of service travelers experience by not having to move their baggage from one mode to the other, particularly over extended distances and periods of time.

To meet such a demand, planners and designers should consider the many issues affecting the various stakeholders involved in providing such a service including, but not limited to: the traveler, the airport and terminal operator, aircraft operators and foreign air carriers, baggage handlers, the other connecting transportation service providers, the Federal Aviation Administration (FAA), and the TSA. It can be expected that the authorized handler(s) of remote checked baggage will be required to seal, secure, and use specific travel routes for moving bags to the airport. Ensuring the remote location can adequately provide for such requirements should be reviewed early in the planning of a remote check-in location. Remote baggage check-in is likely to include operational movements that cut across several airport areas as defined in Sections A through I.

The following is a discussion of some additional considerations associated with providing remote baggage check-in.

1) Remote Baggage Check-In

   Checking and screening bags at the point of remote check-in.

   - The checking-in and screening of airport bound baggage at remote locations can change the requirements for airport and terminal baggage handling and screening in several ways. It addition, it can reduce the demand for screening equipment, screening staff, capacity of the baggage system, and spatial requirements associated with such reductions. Conversely, remote sites will need to include the ability to securely handle baggage that will be screened, sealed, kept sterile, and transported to the airport and terminal. In either case, providing a secure area so that pre-screened bags can be loaded into the baggage sortation system(s), from a single location or multiple locations should be given consideration.
   - Other factors include coordination of assumptions for cut-off times for accepting remote checked baggage; peak hour demands on the baggage system associated with loading significant amounts of remote checked baggage, passenger-bag reconciliation, and storage of early bag check-in.
   - Incorporating such a remote check-in plan should be coordinated with all stakeholders of the remote location to determine the appropriateness of this operating plan, particularly the owner and operator of the remote site. It is essential to identify the chain of custody for remote checked bags when reviewing such a plan with the TSA, and the airport operator. The ability to staff and provide appropriate facilities for the TSA, or an approved contractor, should be assessed early in the development of a remote check-in operation.
   - The spatial program for remote sites is likely to follow those of terminal based locations, including appropriate room for equipment, staffing, all required operations, and ensuring a secure, sterile environment to transfer bags to the mode of travel being used to transport bags to the airport.

   Checking bags at remote point of check-in and moving bags to be screened at the airport.

   - Remote checked baggage can be loaded into the baggage handling and screening process in a number of ways, including a separate baggage screening facility, which will accept remote checked baggage, screen it, and then distribute to sortation devices. This separate facility could be sited at the border of the landside and non-secure areas and the airside, secure, sterile areas. It would include access controls, spatial and equipment needs for screeners and baggage handlers, as well as other standard needs for operating and maintaining a baggage handling system based on the specific in-line screening technology. The capacity of the facility should handle peak hour loads based on remote demands, including provision for multiple bag drop-off loading areas from several remote locations. Consideration for storage of early checked bags should be given.
   - Remote baggage could be loaded directly into the baggage handling system provided the point of entry is secure so the chain of custody is not broken. Once the remote checked bag has been

accepted from the traveler, the opportunity for introducing of any contact with that bag by anyone other than the authorized handler must be precluded. Planners and designers must consider such requirements when planning remote check-in locations, and determining airport curbside, and other terminal and sterile locations for loading remote bags into the baggage handling and screening process.

- In certain markets, remote baggage check-in could occur at several different locations, with different handlers, including some baggage that is pre-screened, and others that require screening at the airport. The ability to handle both conditions should be considered as part of current or future operations.
- It should be noted that this document focuses on the remote baggage check-in issues associated with the airport. Some considerations are provided for the remote site, and it is essential that a coordinated effort by the airport operator, the TSA, and the FAA be undertaken for each remote site before advancing such a plan.

g. Evaluating Design Options

1) Define Performance Goals

The first step in evaluating a design is to identify the functional performance that needs to be achieved from the system. The designers of the system should meet with the airport, air carriers, the TSA, and other key stakeholders to agree on the performance goals.

Items that should be considered include:

a) The timeframe for a bag to be checked-in (or rechecked) by the passenger, transit on the BHS, screened by the TSA, and arrival at the final make-up area(s),
b) The percentage of time the required screening equipment capacity is available for use,
c) Capability and efficiency of the baggage system to queue, track, and convey bags,
d) EDS mean downtime,
e) The time required in the system for OSR to be performed by TSA,
f) Efficient use of staffing resources,
g) Efficiency of design architecture(s), and
h) Availability of the entire CBIS - not just the availability of individual EDS machines or other CBIS components.

2) Determine the Appropriate Planning Horizon

Machine and BHS design requirements should be based on the expected demand over a reasonable planning horizon that accounts for the existing capabilities of the equipment to be used, as well as the future use of existing airport facilities. It is recommended that a design day flight schedule be established to represent the traffic loads.

The flight schedule should reasonably represent the expected loads when the system is expected to be in full operation. This is an important step in the design process: if the expected flight activity is underestimated, then the system will likely not meet the goals during actual operations. If the projected flight activity is overestimated, then the system may be over-designed, and not make good use of the available space and funding available to develop the system.

Over the accepted planning horizon, some annual growth over current flight activity is generally considered to be reasonable, at least to estimate demand levels when the system will become operational. When projecting future demand, planners should also consider possible technological and protocol changes that will impact future processing, throughput, and alarm rates.

3) Evaluating the Performance of the Proposed Solution

It is recommended that advanced planning tools such as spreadsheet analysis, queuing formulas, or simulation models be used to evaluate the performance of the entire CBIS. Through the use of these tools, many aspects of the system can be evaluated, including the number of EDS machines, ETD

machines, and overall baggage handling system requirements needed to best achieve the performance goals for the system.

The choice of the analytical tool should be based on which tool most cost effectively can quantify the performance of the proposed system, or proposed design alternatives, relative to the system performance goals established for the project.

Spreadsheet analysis and queuing models are most appropriate for identifying initial system requirements, or evaluating simple systems.

For complicated systems, including all in-line applications, it is recommended to use simulation models that can estimate peak queue lengths, account for the variability of the baggage handling and screening processes, and incorporate the interaction of bags with each other and the baggage handling system.

Section III-E-2 - Baggage Screening Checklist:

- ☐ **Applicable Regulations**
  - Regulatory Requirement
  - TSA Protocols
- ☐ **Protocols and Concept of Operations**
  - Checked Baggage Screening Options
    - Category 1: Fully Integrated In-Line Systems
    - Category 2: In-Line Systems
    - Category 3: In-Line or Ticket Counter Mounted Systems
    - Category 4: Stand-Alone EDS
    - Category 5: Stand-Alone ETD Systems
    - Category 6: Emerging System Technology
  - ETD and EDS Key Performance Characteristics
  - Design Goals
    - Schedule Issues
    - Fail safe Screening
    - Maximizing Automation
    - Baggage Handling
      - Minimizing Baggage Delivery Time from Check-In to Make-Up
      - Diversion of Out-of-Gauge Bags
      - Oversized Bags
      - Diversion of Alarmed Bags
      - Handling of Selectee Bags
      - International Connecting Bags
    - Capacity Concepts
    - System Maintainability
    - Ergonomics
    - OSRF
    - CBRA
    - Suspect Bag Removal
    - Contingency Plans
    - Environmental Impact
    - Communications
    - Engineering Issues
      - Maintenance Access and Removal
      - Floor Loading
      - Systems Integration and Operation
    - ADA
    - CCTV
      - Surveillance
      - Operational
- ☐ **Design Mitigation**
  - Lessons Learned
    - Avoid Steep Conveyor Slopes
    - Manage Belt Speed Transitions to Avoid Tracking Loss
    - Photo Eyes Too Close to the Belt
    - Avoid Placing Photo Eyes Too Close to Conveyor Ends
    - Avoid Static-Plough and Roller Diverters
    - Use Conveyor Brakes and VFD
    - Avoid Inaccurate Pusher Operation
    - Avoid Improper Merging and Too Many Merges
    - Avoid 90 Degree Merges
    - Avoid In-Line Decision and Removal Points
    - Avoid Directly Opposing Diverters
    - Lack of Decision Point Fail-Safe
    - Avoid Re-Insertion Points Between EDS and Decision Point(s)
    - Avoid Bottlenecks
    - Avoid Using Plexiglas Photo Eye Guards
    - Avoid Short Reconciliation Lines
    - Avoid Non-Powered Rollers
    - Avoid Power Turns at the EDS Exit
    - Use Tubs When Appropriate
    - Consider How Bag Orientation to EDS Will be Maintained
    - Use Caution with Draft Curtains
    - Avoid Tracking without Real-Time Belt Speeds
    - Inefficient Baggage System
    - Efficient Baggage System
- ☐ **Impact of Various Threat Levels on Screening Operations**
  - Temporary space for baggage staging
  - CBRA search area(s)
  - Suspect bag retention and removal area
  - Reasonable vehicle access (e.g., Tug, pick-up, police vehicle)
- ☐ **Alternative Screening Options (Remote Screening)**
  - Remote Baggage Check-In
- ☐ **Evaluating Design Options**
  - Define Performance Goals
  - Determine the Appropriate Planning Horizon
  - Evaluating the Performance of the Proposed Solution

3. Cargo Screening

a. Introduction to Cargo Security

The Aviation and Transportation Security Act (ATSA) directed TSA to implement measures to enhance the security of air cargo transported in both passenger and all-cargo aircraft. In discharging this responsibility, TSA conducted analyses of internal and external threats, risk and vulnerability assessments, and security measures already in place. Proposed rulemaking would require the adoption of security measure throughout the air cargo supply chain; these security measures will be applicable to airport operators, aircraft operators, foreign air carriers, and indirect air carriers. This effort is on-going and likely to continue and affect planning and design considerations in the future. Early coordination with all stakeholders involved in a specific project at an airport, as well as the TSA Federal Security Director responsible for the airport, to ensure all security requirements and concerns are addressed is recommended.

b. Airport - Cargo Processing Facilities

Many cargo security controls present in the supply chain take place prior to the arrival of cargo at an airport facility. In fact, about 80% of all cargo transported on passenger aircraft arrives at the airport from Indirect Air Carriers (IACs), who have their own distinct and extensive security requirements for cargo. In addition to those security controls applied by parties prior to the arrival of the cargo at the airport, further security safeguards should be planned for at, and immediately around the airport itself.

The location of a facility is an essential element to be considered when planning cargo facility design. Because security control requirements for facilities within and part of the airport perimeter are generally more stringent than those required for off airport facilities, serious evaluation should be given to the placement of cargo facilities within the airport perimeter whenever possible. In the interest of maximum security value for the cargo facilities located off airport it is suggested those facilities adopt security controls equal to or above those applied to on-airport facilities.

c. Operational Considerations

At many airports, cargo operations increase at times when passenger movements decrease – such as late evening and early morning hours. Therefore during planning, consideration should be given to facility security on a "24/7" basis. Such items as adequate ramp and exterior lighting should be planned for. If possible during the airport design phase take into account the business of airport tenants. For example, U.S. Postal facilities requirements will vary from a small package acceptance counter operated by a commercial carrier, which will differ from a large all-cargo carrier sort center. Facilities should be designed to allow for expansion of current and future operational practices - such as an increase in the amount of cargo screened by aviation personnel. The ability to identify authorized individuals versus unauthorized persons should also be taken into account. Personnel movement (both employee and customer) should be thought of as well as volume and size of vehicle movements from and in the public side so as to minimize any disruption to the pace of operations. Additionally, consideration should be given to allow for the security of a building in an emergency situation.

Cargo buildings which are part of the airport perimeter should be secured so that they are adequately protected against unauthorized entry. The ability to significantly limit the immediate access (due to such circumstances such as an increase in the national terrorism threat level) to the AOA, secured areas, and areas which are used to store and stage cargo should also be planned for. Creating access points on the public side of buildings thereby making the interior of the facility itself a controlled area should be considered. Requiring contractors and customers to utilize a separate entrance from employees should also be taken into account. Airport designers should determine the applicability of a staging area for the contractors to drop off cargo but limits their access to the facility. The use of emerging technology such as biometric security systems should be considered when evaluating employee/ contractor access points. Security cameras should be given consideration for surveillance in areas controlled for security purposes as well as other areas of concerns where cargo movement occurs; the need to prevent tampering, theft or to meet continual control requirements may be facilitated through such systems. Security cameras provide additional benefits by identifying threats, detecting unauthorized access, the assistance of emergency response units and as a deterrent for theft.

d. Access Control Considerations

Cargo facility access points must be capable of being secured when not in use in order to prevent unauthorized access. When cargo doors, gates or other access points must be kept open (such as for ventilation), controls must still be in place to prevent unauthorized access. For instance, a lockable fence could be used to allow for increased ventilation and also secure a vehicle access point into a warehouse normally secured through a roll down garage door type barrier. Electronic intrusion detection systems (augmented by appropriate alarm assessment and response capabilities) may be an option as well.

Personnel doors used by employees as primary access points to cargo buildings should be located so that they can be controlled and secured when required. In order to facilitate ease of monitoring consider limiting the number of entry points for employees. For large cargo facilities consider parking or drop off areas for employees. Security is more easily applied when only 20 buses have access to a restricted area rather than 500 individual cars. Location of these facilities may require the transporting of employees through active aircraft parking and movement areas requiring operational authorization not normally granted to personal vehicles. When considering employee facilities, consider the distance of the parking to the facility.

Consideration should be given to building designs that would eliminate the need for fencing. For example, when a facility is used as an air side perimeter barrier, consider attaching the building to a terminal or another cargo facility. Where fencing is utilized, take into account the lifespan of cargo fencing exposed to vehicle misuse in high traffic areas. This may be extended through the use of properly placed curbing, bollards, or highway railing. Fencing should be secured at the bottom as to prevent lift up and intrusion. Landscape should also be accounted for when constructing a new facility. Landscaping design which could unintentionally allow for concealment of unauthorized persons or items at areas immediately adjacent to the public side of cargo facilities should be avoided whenever possible.

Operations within cargo building should also be taken into consideration when designing airport facilities. Cargo handling and control must be measured in the overall allocation of space and manner of transit from cargo make-up to aircraft loading. This might include space for bulk pallet inspections, and secure cargo hold areas. The ability to easily distinguish between public and non-public areas within a building will allow for ease in distinguishing authorized and unauthorized personnel. Space should be considered for documentation and storage requirements, as well as general administrative needs accomplished by administrative staff. These actions are separate from the storage and screening of the cargo done by an operational employee. As the amount of air cargo screened increases due to government requirements and/or industry initiatives additional facility space may be needed to accommodate additional screening. Planning should take into account any equipment that may be used for screening as well as the footprint and personnel the equipment may dictate. Some equipment does not function properly in the adverse climate that is sometimes found in cargo buildings. Consideration should be given to the location of the equipment within the cargo facilities and the possibility of creating a protective and secure environment area within the facility. Equipment should not be placed in areas that could disrupt operations or increase the likelihood of damage from operational procedures. The facility should be able to expand with the addition of manpower, cargo holds, clearance, separation of cargo and or in-line screening systems.

e. Information and Requirement Resources

The Federal Security Director should be consulted when designing cargo facilities. Federal Security Directors have first hand knowledge of the security needs and requirements specific to their airports. Federal and/or local authorities may develop and disseminate information that would require preplanning by the airport or the aircraft operator to carry out additional security measures intended to respond to an elevated threat.

Section III-E-3 - Cargo Screening Checklist:

- ☐ **Access points addressed**
- ☐ **Access points for employees/ contractors**
- ☐ **Space for additional technology, staffing requirements**
- ☐ **Sorting areas, separate from acceptance areas**
- ☐ **Separation and security of cargo prior to and post inspection**
- ☐ **Accessibility of building to commercial entities/ employees**
- ☐ **Perimeter needs**
- ☐ **Facilities for employees**
- ☐ **Postal facility inclusion**
- ☐ **Emergency response factors**
- ☐ **Inclusion of specialized personnel in determining security concerns**

Section F - Access Control and Alarm Monitoring Systems (ACAMS)

In addition to the airport operator's Access Control and Alarm Monitoring System (ACAMS), airports often involve other tenants and agencies with independent, and frequently differing, ACAMS needs and/or requirements. Consideration should be made early during any project's planning and design phases to evaluate the benefits, needs and feasibility of independent versus integrated ACAMS (and CCTV) equipment. The level of integration can vary from solely monitoring/status capability to full single-system functionality, and has cost as well as operational and security implications. The decision may also depend to some degree on the proximity of the facility to the airport operator's own areas of security interest, passenger enplanement facilities, and the agreement between the airport operator and tenant as to the demarcation of responsibilities.

Technical details concerning many elements of airport access control systems discussed in this section are available in the RTCA Airport Access Control Systems Standard 230A (An update to this document, Standards 230B, is currently underway).

1. Suggested Support Requirements

a. Nature and purpose of ACAMS systems

Airport access control systems (ACAMS) are systems to control the passage of staff (not passengers) into secure and sterile areas in line with the regulatory requirements of 49 CFR 1542 et al and the airports specific ASP. These systems are not designed to control the access of passengers and specifically not for the "Trusted" or "Registered" travel program.

b. Regulatory requirements overview

In addition to the regulatory requirements, these systems are also the subject of a number of security directives which describe special requirements. For security reasons these special requirements are not described in this document. Such requirements can be obtained on a need to know basis only from the Federal Security Director associated with the airport in question. Note that general aviation (GA) only airports do not normally require access control systems. Security guidelines for general aviation airports are, however, available.

c. Other standards

This section only outlines the requirements and provides general guidance. There are three other sources of information for the design of access control systems: namely (1) the RTCA 230 standard which specifies technical standards for operating systems, and (2) the Airport Security Policy and Guidance handbook only

available from the TSA on the same conditions as the Security Directives listed mentioned above, and (3) the TSA Guidance Package – Biometrics for Access Control dated 31 March 2005 which is publicly available.

Biometric identification is emerging as a critical feature of security systems. Passports containing biometric identification data are now being issued for international travelers, and this trend will increase as nations agree on what biometric means are to be used and how the resulting data are to be protected from abuse. This trend will impact airports - the ICAO has already declared its preference for facial recognition, with iris scan and fingerprints as backup, and U.S. standards for staff access control can be expected once the results of TSA biometric evaluation pilot programs are evaluated.

The following sections are taken from the TSA biometric Guidance Package, which all airport planners and designers concerned with access control security, should read and taken in account in their planning.

This guidance package addresses biometrics for airport access control. Access control addresses the examination of one or more of three factors regarding an individual's identity: something they know, something they have, or something they are. Biometrics is the field of technology devoted to identifying individuals using biological traits or "something they are." It uses automated methods of recognizing a person based on one or more physiological or behavioral characteristics.

On December 17, 2004, President Bush signed into law the Intelligence Reform and Terrorism Prevention Act of 2004. The legislative language of this act in Title IV – Transportation Security, Section 4011 – Provision for the Use of Biometric or Other Technology, directs TSA to "issue, not later than March 31, 2005, guidance for use of biometric technology in airport access control systems." TSA provides this guidance document for airport operators to use to improve upon their existing access control systems by incorporating biometric technologies. Such improvements are not required.

Regulations governing airport security: These are found in 49 CFR 1542 requires airport operators to adopt and carry out a security program approved by TSA. Specifically, airport operators with a complete program must, among other items, ensure that its security program defines how the airport will:

- Establish a secured area – Air Operations Area (AOA) and/or Security Identification Display Area (SIDA);
- Control entry into the secured area via access control systems; and
- Perform the access control functions required and procedures to control movement within the secured area, including identification media.

A majority of airports in the U.S. fall under the Part 1542 regulations and thus have some type of access control system for their secured areas. Currently, very few of these airports have access control systems with biometrics, some of which were implemented through TSA pilot programs at a limited number of access points.

Section 4011(a) (5) of the Intelligence Reform and Terrorism Prevention Act (the "Intel Bill") directs the Assistant Secretary of Homeland Security (TSA), in consultation with representatives of the aviation industry, biometric identifier industry, and the National Institute of Standards and Technology (NIST), to issue guidance to establish, at a minimum:

(A) comprehensive technical and operational system requirements and performance standards for the use of biometric identifier technology in airport access control systems (including airport perimeter access control systems) to ensure that the biometric identifier systems are effective, reliable, and secure;

(B) A list of products and vendors that meet the requirements and standards;

(C) procedures for implementing biometric identifier systems to ensure that individuals do not use an assumed identity to enroll in a biometric identifier system and to resolve failures to enroll, false matches, and false non-matches; and

(D) Best practices for incorporating biometric identifier technology into airport access control systems in the most effective manner, including a process to best utilize existing airport

access control systems, facilities, and equipment and existing data networks connecting airports."

The TSA guidance is primarily directed to two groups: (1) airport operators, who own and operate the access control systems at their airports; and (2) manufacturers of biometric devices, who need to submit their devices for qualification (including performance testing) in order to be potentially placed on a TSA biometric Qualified Products List (QPL). A major component of the TSA guidance is to provide criteria that a manufacturer of biometrics devices will be expected to meet in order to have itself and its device(s) included on the QPL. Manufacturers will find this TSA guidance crucial to understanding the technical and operational requirements that their biometric devices should meet and the standards to which they should conform. (Note that as used in this document, the term "airport operators" may also include other organizations/subcontractors designated and approve to perform access control administrative functions.)

Airport operators who choose to incorporate biometrics are encouraged to use this guidance to procure and integrate the biometric component into their legacy (i.e., existing) access control systems and to update their airport security programs. The end users of biometric access control systems are airport, air carrier and airport tenant employees, who access secure areas of airports.

Figure III-F-1 below provides a graphical view of the relationship between the airport access control system (as a whole), the biometric sub-system boundary, and the biometric device. Note that *Figure III-F-1* is a generic diagram and that specific implementations may vary from this particular depiction.

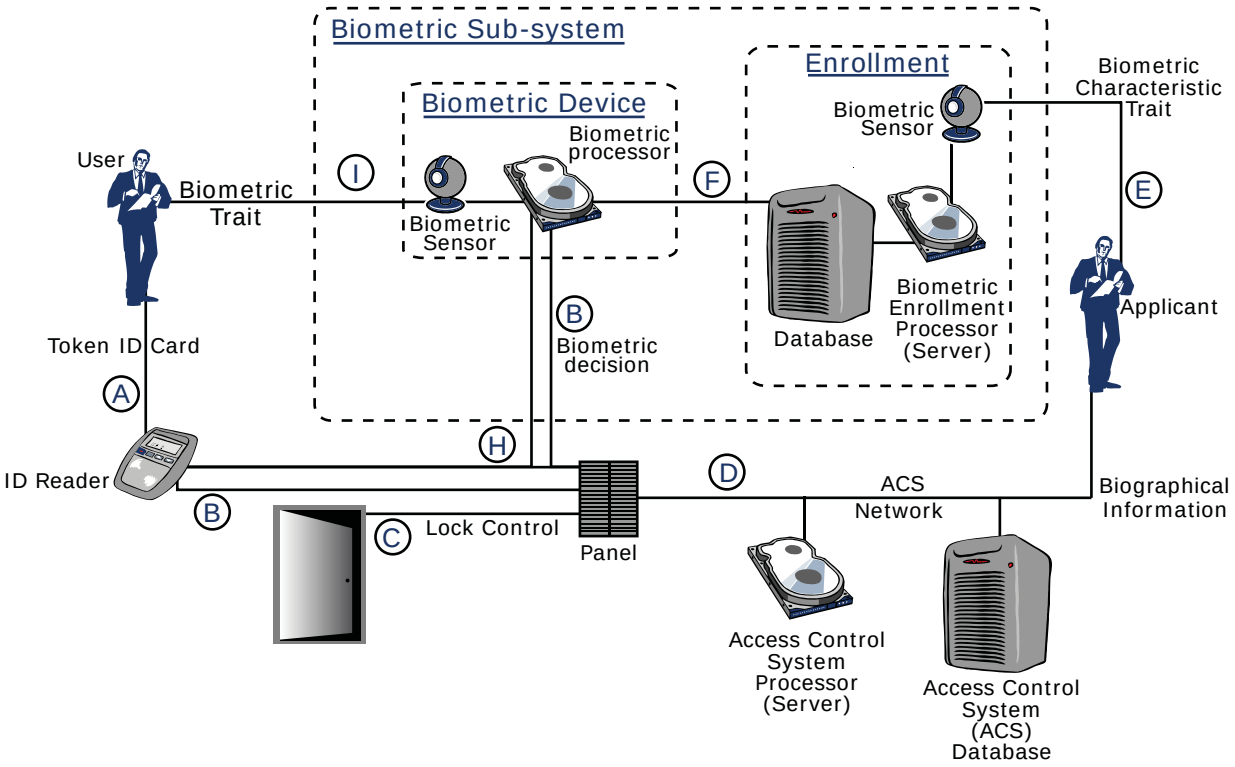


Figure III-F-1 - Generic Biometric-Based Access Control System

2. Operational Requirements

a. Primary Roles

In general access control systems have three roles: to monitor access to the secure and sterile areas, to annunciate any security violations and to record and log events. Normally at all but the smallest airports this is achieved by an electronic access control system.

b. Monitoring

The prime purpose of access control systems is to control access by authorized staff (of various types) to secure and sterile areas. This is typically done by means of an identity access media or combined access/ID media card which is presented to a card reader at a portal.

The system verifies that the holder of the access/ID media is entitled to pass through the portal and either unlocks it to allow passage, or denies passage and provides a local indication of this denial. The same access/ID media can be used at staffed security portals such as vehicle gates.

Note that it is not a requirement of such systems to monitor and control all access points. Some infrequent use access points can be secured by conventional means, e.g. padlocks.

Most airports also use such access system to control access to AOA areas not designated as secure areas, and also to administrative areas. This is not a regulatory requirement.

c. Annunciating

The annunciation function is similarly simple. It is to annunciate whenever persons enter secure or sterile zones without permission and also to annunciate whenever repeated attempts are made to enter an access point in the face of a denial. This annunciation can be accomplished locally by means of a local alarm, and remotely at a "dispatch" or control center monitoring the alarms and capable of dispatching appropriate personnel to the scene of the breach or attempted breach.

d. Recording

The recording function is to record and automatically log all attempts to enter secure and sterile area as appropriate, whenever successful or unsuccessful.

e. ID/Access Media Management

The system should provide means to manage the ID/access media issued to staff and to control their rights to access certain doors, can limit these by location and time, and restrict the duration of the validity of the card. Such ID/access media should only be issued to staff following the successful completion of the required background and security checks.

These requirements are described further in sections below. The system should be capable of almost immediate repudiation of a ID media holders access rights, partially or completely on request from an authorized person, typically airport security staff or the TSA.

f. Performance criteria

Airport security systems should be high availability systems operating 24/7/365. System availability should meet or exceed 99.99%: higher performance requirements should be considered for higher risk airports. Detailed performance and maintenance criteria are in the RTCA 230 document referenced above.

g. Security zone area support requirements

At present the airports are divided into a number of zones areas by the current regulations. These are subject to change. The current security zones are Sterile, Secure, SIDA and AOA. Cargo areas are also included depending upon their location within the security areas. The system should support the control and monitoring of access to these areas and should also be capable of supporting additional areas which may be so designated by regulation or the TSA.

3. On-Site Communication Requirements

In general, on-site communication requirements of access control systems at airports have two components, the requirement to link the devices at portals to local control panels (secondary or horizontal wiring) and the

requirement to link these devices back to a central server (vertical, backbone or primary wiring). Note that this subject is covered in detail in the RTCA access control systems standard 230A.

a. Backbone Infrastructure

Current access controls systems, with the exception of the smallest, use a standard IP based backbone communication structure. Legacy systems use a variety of techniques. These will be covered in section 7 below. As such new systems can easily share a common communication infrastructure (see the *Power, Communications and Cabling* section on page 180) for communicating between the main server, which typically holds the access control data base and the local communication controllers.

b. Secondary Infrastructure

Current access systems are in a transition phase. Most systems currently available use proprietary standards and legacy communication systems from local control panels to devices and door controllers. As a result they typically cannot share a common communication infrastructure.

However, new systems which use an IP based secondary communication structure are coming onto the marketplace. These could share a common infrastructure if such was extended to the secondary distribution. Note that not all facilities have such a common secondary infrastructure.

c. Use of shared communications infrastructure

The current RTCA standard 230 specifies specific requirements in this regard. These indicate how the use of a common infra-structure should be deployed so as to maintain a high level of security appropriate for ACAMS systems. Essentially this allows the use of shared cable but requires physical separation of control of the fiber and copper. Technical details are to be found in this the RTCA standard.

d. Use of common and shared networks

The Current RTCA standard specifically recommends against the use of shared networks for access control systems except for special reasons. This is 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 less and have separated out the applications by VLANS and the like, at the cost of some increased administrative complexity.

e. Use of wireless technologies

Wireless technology is convenient and often less expensive to deploy than conventional technology. But it has inherent risks. Any omni-directional transmission, in which the majority of Wifi type systems are included, is at risk from a denial of services attack, even if the best possible security and encryption measures are deployed. Thus, wireless transmission should not be used for critical transmission wherever possible.

Point to point uni-directional links 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 in all weather circumstances. These issues are under review for the next version of the RTCA standard 230.

f. Maintenance considerations

Modern communication technology offers a wide choice of devices and options. However these can come with a maintenance and administration administrative complexity. Smaller airports may wish to consider if this complexity is worth the benefit that these system bring.

4. Power Requirements

In general, access control systems have three power requirements:

- At the server
- At the local control panel
- At the portal

Each requires power to operate. This power should be provided via a UPS, and be connected to backed-up power to ensure continuous operation even during a power failure.

a. Server/head end

Servers are usually located in a main equipment room which has backed up and UPS power. ACAMS servers and communication controllers do not require large amounts of power but their requirements need to be factored in to the total power requirements. A UPS for a processor should provide at least four hours of system service.

b. Local device controller

Local Device controllers are usually located in communication closets. Most local panels run on their own local power supply with a built in UPS. The load is typically not large.

c. Device power requirements

Door and portal devices are of two types, those which require little power, such as door sensors and card/ID media readers, and those which require more power such as magnetic locks. (Vehicle gates are another category and are discussed in *Airport Layout and Boundaries* on page 13). Depending on the system the power, typically 24VDC is either generated locally from a backed up supply or centrally at the nearest closet via a UPS. Magnetic locks and the like have a significant power use and provision of a UPS capability of any reasonable time duration is a design issue.

Conversely, the power requirements of sensors and ID media readers is such that techniques such as power over Ethernet could be applied if the device were on IP based communication, (which many are not) otherwise conventional low voltage wiring from the communication closet can be deployed. See the RTCA standards document 230 for more details.

5. Credential Access Media Requirements & Issues

a. Existing access media

Most airports still use magnetic stripe or proximity technology credentials. The technology in this area continues to evolve and improve. The airport, the design and planning team, and the local FSD should evaluate the existing access media to determine whether change is needed and what new media should be incorporated in the overall airport security system.

b. New federal credential standards

The situation with regard to federal standards for credentials is still unclear. This issue is being addressed by the committee that is currently updating the RTCA standards document 230A. In the meantime, there are two sources of standards for government credentials, namely the GSC-IS V 2.1 standard and the FIPS 201 standard. Neither is mandatory at the time this document was published but may have become since. Support of the latter would probably require an IP based communication link from each reader.

c. TWIC program

The TSA has had a TWIC pilot program underway to support a nationwide identity credential. No reports have yet been published of its results. If this program goes ahead it will require on line links back to a TSA data base, a card probably compatible with FIPS201 and a biometric reader. However, at present there is no regulatory requirement or security directive requiring same.

d. Biometrics

Biometrics is an additional form of authentication of an individual. They are a requirement at the higher security levels of FIPS 201 and the GSA specifications. There is no current regulatory requirement for biometrics, but some airports have chosen this option. Additional guidance on this issue is provided in the TSA guidelines for biometrics at airports and the RTCA standard.

Note that installing biometrics at each portal will may potentially require the installation of an additional IP capable link to that portal.

e. Environmental requirements

If the airport access control system is to be used outside, and not just inside a facility, attention should be made to local environmental constraints, such as ambient temperature, lightning, wind, sand, snow and salt spray. These would have an impact on both the type of credential and the biometric which could be deployed: in many cases the performance of the reader and credential is impacted negatively. This issue is covered further in the RTCA standard 230.

6. Identification Systems Requirements

a. Regulatory Summary

There are specific requirements in 49 CFR 1542 relating to the issuance of security access credentials at airports. These regulations are supplemented by a number of security directives. The details of which are omitted here for security reasons. These regulations include verification of identity, CHRC either manually or via the Transportation Security Clearing House clearing house, and comparison against updates and check lists produced regularly by the TSA.

b. Required links to federal systems

There are no direct links required at this time between ACAMS and federal systems. However larger airports currently use commercial "live scan" fingerprint systems to link into the "clearing house" set of systems maintained under federal contract by the Transportation Security Clearing House. These fingerprint systems need to be provided with secure access to this system via public networks. Note that some states have additional requirements, for example transmission to local Departments of Justice.

c. Identification (ID) media system operational requirements

At larger airports some identification (ID) offices have such a high turn over (a.k.a. churn), or an inherently high transaction rate, that they resemble state Department of Motor Vehicles offices. If an airport has such a transaction rate then similar special facilities, including queuing and multiple service counters need to be provided. At smaller airports credential requirements are often minimal and a single workstation usually suffices.

7. Special Device Considerations

a. Anti-tailgating devices

The purpose of anti-tailgating devices is to stop people and vehicles tailgating through a portal. Vehicle anti-tailgating measures are covered in *Airport Layout and Boundaries* on page 13. Personnel anti-tailgating devices are of two types:

- Anti-tailgating devices such as turnstiles specially manufactured for that purpose
- Additional general-purpose sensors/devices attached to existing portal

Devices are typically interfaced into an ACAMS system in a conventional manner. However, in contrast, additional devices usually require additional add-on equipment and processing in order to effectively detect or deter a "tailgate". Several systems based on video analysis may need operator interpretation.

b. ADA issues

A subset of the access portals at any airports are required to be ADA compliant. This requires additional equipment at the portals and additional clearances. In addition some states have additional requirements, over an above that specified in the ADA regulations.

c. Fire door and Emergency exit issues

In general it is not good practice to have a fire door regularly used as an operational door. However, certain terminal topographies make this difficult to avoid and still remain within local fire codes. Included in these measures are crash bars linked to the ACAMS system to detect operation of these doors. This is especially important on fire doors which give access to secure areas and the AOA. (See *Terminal* on page 58 for further discussion of fire doors and emergency exits)

d. Elevators

Elevators should, all other things being equal, not allow access from public to secure areas. Unfortunately this is not always possible, and dual use elevators are not uncommon. In the event of dual use, the controls to access the secure and sterile areas need to be under the control of the ACAMS wherever practical. In addition, airports should consider occupancy detection, so that an elevator cannot be boarded at a public floor and then brought down to a secure floor with a passenger without warning or positive controls.

e. Environmental requirements

Use of access control systems inside facilities has presents minimal environmental issues. Use outside or in exposed baggage handling areas with dirt, dust heat and or snow is an issue. Devices and credentials should be selected accordingly As of August 2005 the HDS transportation Security Laboratory is completing the "20 airport Access control projects" as mandated by ATSA. This should give additional information on this issue. The RTCA standard 230 covers these requirements.

f. Legacy system integration

Except in some completely green field sites there will almost certainly be some form of legacy system at some locations which should be interfaced to a new ACAMS system. Interfacing of such systems can be complex and is covered in the RTCA standard. In general however, the simpler the interface the better.

8. Federal Inspection Services (FIS) Device Requirements

a. Special security requirements

FIS Areas form another category of security area. The requirements for security, and the delineation of these areas, are described in detail in the CBP publication: Airport Technical Design standards. These requirements are for the separate securing and monitoring of the inspection area, and the passageways to and from the incoming international aircraft to this area.

b. Special command and control requirements

These are enumerated in detail in the CBP publication referenced above which lists the locations at which the alarms should be monitored, normally the CBP Coordination Center, (previously often known as the Joint Agency Coordination Center). However, it should be noted that most of the security requirements in this publication are met by most modern access control systems, and by any system conforming to the RTCA standards.

One specific difference from the existing regulations, but not current practice, is to require CCTV coverage on both sides of the doors entering into the CBP "sterile" area. In addition, the CBP agency requires additional access control on its internal offices within this area. This is again in line with current practice.

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

c. Additional details

For additional details, see *International Security* on page 191.

9. Integration with Other Systems

Security systems with which access control integration is typically required include CCTV, Perimeter, Duress Alarms, and others identified below.

In addition to the design and technical characteristics of physical security systems, airports and their architects-engineers must also address issues of access to and the release and dissemination of security operational and event information. Much security event data will be treated as Security Sensitive Information (SSI) at the federal level, with restrictions on access and public release including possible restrictions on access by airport security personnel. Some information, particularly video imagery, may also raise privacy issues with

corresponding restrictions on sharing and/or releasing such imagery to the public. These operational and procedural issues should be addressed by airports in formulating their Airport Security Plans.

a. CCTV

CCTV is widely used in association with ACAMS systems in order to effectively monitor an access portal. Details of video surveillance requirements are given in *Video Surveillance* on page 162. From an access control system point of view there are three main requirements:

1) The CCTV cameras must be located to give as good a view as possible over the each portal, so that it can be monitored effectively. Selection of each location and camera type depends on operational mode and local topology.

2) The CCTV system should be linked with the ACAMS such that when an alarm or other identified event occurs the video from the CCTV camera(s) are automatically switched on and the video presented at the appropriate monitoring location. (See subsection 11 below for dispatch requirements.)

3) The video system should not only annunciate this alarm but also record the video clip(s) associated with each alarm and store and name these clips using the same name as the access control event so as to ease facilitate latter recovery of the clip. This name should be meaningful and related to the event. The video system should automatically switch to its highest frame rate for this clip. The duration of this clip should be configurable per portal.

4) Issues related to the sharing and release of video imagery taken by security cameras are addressed in *Video Surveillance* on page 162.

b. Perimeter Intrusion Detection systems (PIDS)

Perimeter intrusion systems are typically found on the airfield perimeter. These can be monitored by a separate system but most airports have chosen to link these into a single system for convenience purposes. Numerous perimeter intrusion technologies are available. See *Video Surveillance* on page 162 for further details.

c. Duress alarms

Duress alarms can be installed at various locations throughout an airport. This includes checkpoints, on which see below, but could also include dispatch offices, and even the check-in and ticket counters. Location and installation of these devices is airport and operational model dependant. These devices are usually linked back into an ACAMS system to provide a common annunciation point for operational effectiveness and convenience.

d. Vehicle gates

Vehicle gates are described in detail is *Airport Layout and Boundaries* on page 13. Because of the regulatory requirements and security directives associated with security gates, there is a clear requirement to link these back to the ACAMS system to provide the same level of control as at normal portals. Other special considerations apply which are covered in *Airport Layout and Boundaries* on page 13.

e. EDS support: TSA and EOD support

Some airports have chosen to install ACAMS devices in EDS areas and EOD areas so as to secure the areas and prevent theft and interference with equipment. This decision is based on local conditions and operational practices.

f. Checkpoint breakthrough control

Design issues associated with the Security Screening Checkpoint are covered in detail in *Security Screening* on page 87.

From an ACAMS point of view a potential application at a passenger screening checkpoint is that in the event of a breakthrough, or other event, at a passenger screening checkpoint is that the associated concourse portals can be promptly secured. The ability to achieve this depends on the concourse's topology and local fire codes.

The objective is to automatically shut and secure all doors leading from the concourse to secure areas and to office space. This radically reduces the area which has to be evacuated and searched in the event of such an incident.

In addition, depending on concourse layout, it may be appropriate to automatically partition the concourse, by means of automated doors etc, so as to further restrict area required to searched/evacuated as required. Placement and design of such doors need to be carefully coordinated with local fire codes and ADA requirements.

g. Integration risk reduction

Integration between systems has proven to be one of the most problems problem-prone areas of airport security from a technical point of view. Some of these problems have been caused by an over enthusiasm with technology and an underestimation of implementation issues.

10. Command and Control Requirements

For technical requirements on integration see the RTCA access control system standards document. CBP monitoring locations are covered in section 8 above.

a. Monitoring locations

An access system is required to be monitored at some location so that appropriate responses can be made to alarms, and staff and resources dispatched accordingly.

There is typically a control and command center of some type, often called an SOC or Security Operations Center. This center can be located either located in the facility being monitored, or as is more normal, centralized at one location for an entire airport. Typically, at these locations, not just access control, but CCTV and other systems are monitored. See *Terminal* on page 58 for further discussion of this issue.

b. ACAMS Administration and management locations

In addition to the monitoring and dispatch locations there is a need to have a location identified from which the ACAMS system can be administered. This need not be in the control center. At smaller airports it can be located in the identification (ID) office.

c. Primary and Alternate Operation centers

Because of the importance of the dispatch center, several airports have chosen to implement two such centers and primary and an alternate to use in the event that the primary is not available for whatever reason. The alternate center need not have the same scale as the primary center but should have the same system connectivity to access control and other systems.

11. Design Process Outline

ACAMS systems at airports are unusual in that they are effectively closely regulated. The current conventional design process includes:

- Operations requirements definition
- Conceptual Design
- Detail design
- Implementation
- Commissioning

Other specific issues which must be considered as parts of design include ASP and AEP; security boundaries placement; and technology choices.

a. ASP and AEP

The security operations of any regulated airport is described in a TSA approved ASP, an SSI protected document.

Access control is a significant part of this plan. If an airport already has an ASP, then any new facility's security provisions should, under normal circumstances, be in line with this document.

In addition, most airports also have a specific AEP as required by 14 CFR Part 139. Again if an airport already has an AEP, then any new facility's security provisions should, under normal circumstances, be in line with this plan.

b. Security Boundaries Placement

A key issue in the deployment of security measures is the accurate predetermination of security boundaries for the various security zones as specified in the regulations. These include the:

- Secured area
- Sterile area
- AOA

If CBP facilities are included in the project, the boundaries of this area also need to be planned.

c. Technology Choice

The selection of technology for access systems is complicated by two factors:

- The uncertainty with regard to the technologies and standards that will be regulatory may be required in the future
- The state of the industry is currently in rapid flux and offers a variety of options.

Given that an airport access system typically lasts less than 10 years before replacement, significant care and attention needs to be given to the choice of supplier, credential and supporting infrastructure to support a system for that duration, without replacement.

For all choices of equipment there should be a balance between cost, security and functionality and flexibility/expandability.

Section III-F - ACAMS Checklist:

☐ **Power Requirements**
- Emergency power systems/battery back-up for servers
- Emergency power systems/battery backup for control panels
- Emergency power systems/battery backup for operating stations
- Emergency power systems/battery backup for door hardware

☐ **Data and Communications requirements**
- Sever to panel communications
- Panel to door communications
- Server to dispatch area requirements
- Wherever possible a security network should run on physically separate dedicated and protected systems from non-security systems.

☐ **Security System Infrastructure**
- Separation from non security infrastructure
- Controlled access
- Access for maintenance
- Secure access for management

☐ **Potential Equipment Placement Locations**
- Terminal Area Access Points
  - Secure area access Personnel Doors
  - AOA access Personnel Doors
  - Sterile Area Access Personnel Doors
  - Concourse area entrances (grills)
  - Inbound/Outbound Baggage Doors
  - Inbound/outbound Baggage Doors control
  - Loading Dock Doors to Secure/Sterile/SIDA/AOA
  - Service Corridor and Stairwell Doors
  - Administrative Office Doors
  - Telecom Room Doors
  - Maintenance Area/Equipment Room Doors
  - Tenant and Concessions Area Doors
  - Roof Access Points
  - Manhole access points
  - Fire/Emergency Exit Doors
  - Material Storage/Safe Areas
  - Display/Museum/Art Cases
  - Hazardous material storage areas
  - CBP areas
  - TSA offices
  - EDS operation areas
- Terminal Duress/Convenience Alarms
  - Passenger Screening Checkpoints
  - Baggage Screening Areas
  - Ticketing/Rental Car Counters
  - Administrative/Information Desks
  - Companion Care/Family Restrooms
  - Police Substations/First Aid Areas
  - Chapels
  - Concession/Retail Cash Registers
  - Dispatch and communication locations
- Site Access Points
  - AOA/SIDA/Secure Vehicle Gates
  - Maintenance/Personnel Gates
  - Non-Terminal AOA/SIDA Doors
  - Site Telecom Room Doors
  - Maintenance Building Doors
  - Tenant Facility Doors
  - Navaids and FAA facilities
  - Cargo Facilities
  - Perimeter gates
- Site Alarm Points
  - Material Storage Areas
  - Parking Management/Tenant Safes
  - Critical Equipment Locations
- Site Duress/Convenience Alarms
  - Parking Toll Booths
  - Parking Management Office Money-Handling/Storage Areas
  - Public Parking and Garage Areas
  - Ground Transportation/Taxicab Booth Areas
  - Administrative/Reception Areas
  - Tenant/Cargo Cash Register Areas
  - Airport/Tenant Guard Booths

☐ **Dispatch requirements**
- Monitoring locations should be in a secure area
- Monitoring location should be separate from normal offices
- Monitoring locations should be part of an integrated incident dispatch program
- Monitoring locations should have relevant CCTV access capability
- Alternate monitoring capability location should be provided.
- Monitoring location should be separate from admin and identification (ID) locations

Section G - Video Surveillance, Detection and Distribution Systems

Airport planners and designers are continuously challenged by evolving technology during lengthy design and construction projects. Every airport wants to open with modern systems in place, but design and purchasing commitment must be made years earlier. System and equipment specifications drafted during Schematic Design and Design Development can be superseded by new technology and by new standards by the time construction is completed.

This is often the case with the technologies treated in this section - video surveillance, computer networking, and information distribution – where new (and potentially disruptive) capabilities are created on relatively short time cycles. To cope with this situation, designers should systematically monitor technology trends which may impact their systems and determine which near-term developments can be considered for their projects without jeopardizing project performance, schedule, and cost. It is not a simple task, but properly done it can minimize the cost of having to upgrade or replace equipment which may only recently have become operational.

1. Uses and Purposes of 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, operates for years with minimal maintenance, and requires minimal operator training.

CCTV systems are now used at airports for a variety of purposes including:

- Area surveillance in terminals,
- Roadway and curbside baggage,
- Cargo loading docks,
- Tenant access points,
- Baggage handling areas,
- Access points to the SIDA, AOA and other security areas,
- Monitoring passenger traffic inside the SIDA,
- Gate activities,
- Monitoring of fenced perimeters,
- Vehicle traffic control,
- Rental Car Facilities
- Fuel Farm Areas
- Passenger parking garage and parking lot monitoring, and
- Employee parking areas.

2. Operational and Technical Issues

a. Assessment & Surveillance

The performance of a surveillance system depends on a number of factors including the characteristics of the object to be observed (e.g., its size, reflectance, and contrast); local environmental conditions (e.g., atmospheric clarity and scene illumination); camera characteristics (e.g., detector size, sensitivity, and resolution); characteristics of the camera objective lens (e.g., focal length and relative aperture); characteristics of a display or monitor (e.g., resolution and contrast); and the ability of the human eye to resolve target details (which also depends on whether this is done in daylight or at night).

The technical standard for assessing the performance of an imaging sensor is its Modulation Transfer Function (MTF), which measures the spatial frequency modulation response of the imager. MTF can be thought of as a curve, indicating for each spatial frequency the ratio of the contrast modulation of the output image to the contrast modulation of the input image. It is formally defined as the magnitude of the Fourier transform of the line spread function of the imaging system.

MTF is not a practical tool for airport security personnel because of its complexity, because commercial video cameras and lenses rarely disclose MTF performance, and because MTF has no real-world analog, i.e., airport personnel will not be able to relate MTF values to what they actually see.

For airport security, a key issue in establishing surveillance requirements is resolution, i.e., the ability to resolve operationally-significant details at a specified distance. The U.S. military faced the same dilemma in the 1960s when it was developing electro-optical sensors for night operations. The military solution was a set of criteria, known as the Johnson Criteria, which express imaging performance in terms of real-world target characteristics and observer requirements. This solution is still applicable and is taught in the engineering departments of military schools in several countries.

Various levels of target discrimination, each requiring a different amount of "information", were defined by J. Johnson of the Army Warfare Division, Night Vision Laboratory (1966), to be:

1) ***Detection*** - an object is present,

2) ***Orientation*** - the longitudinal axis of the target can be sensed,

3) ***Recognition*** - the class of target can be discerned,

4) ***Identification*** - target types within a class can be determined.

The Johnson Criteria for imaging performance are shown in *Table III-G-1* below for nominal civilian targets with two probability levels of an observer's confidence. The table assumes 2 TV pixels per line pair.

Table III-G-1 - Resolution per Minimum Target Dimension in Line-Pairs

Observer's Requirements	Observer's Confidence Level	Truck or SUV Target	Person - Standing Target
Detection	0.50 0.95	0.90 2.00	1.50 3.20
Orientation	0.50 0.95	1.25 3.00	1.80 3.80
Recognition	0.50 0.95	4.50 8.00	3.80 7.60
Identification	0.50	8.00	8.00
	0.95	13.00	26 for surveillance, up to 40 for legal evidence

The amount of "information" required by an observer increases as the operational requirement progresses from detection to identification, and as the confidence level of the observer in what he or she sees also increases (expressed as a probability value). These relationships are shown in the following table, with the data for military targets in the Johnson tests having been adjusted for the nominal civilian targets shapes.

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 will be in a position to evaluate the proposed design in operational terms.

Resolution is an important performance parameter but it is not the only parameter to be considered in establishing system requirements. Field-of-view, also known as angular coverage, should also be addressed, especially for fixed video cameras.

In Figure III-G-1 below, the black bars represent "line-pairs" across a critical dimension of the target which relate to the probability that an observer can detect or recognize the target. For modern solid-state video cameras, a line-pair is equivalent to two pixels of the detector array.

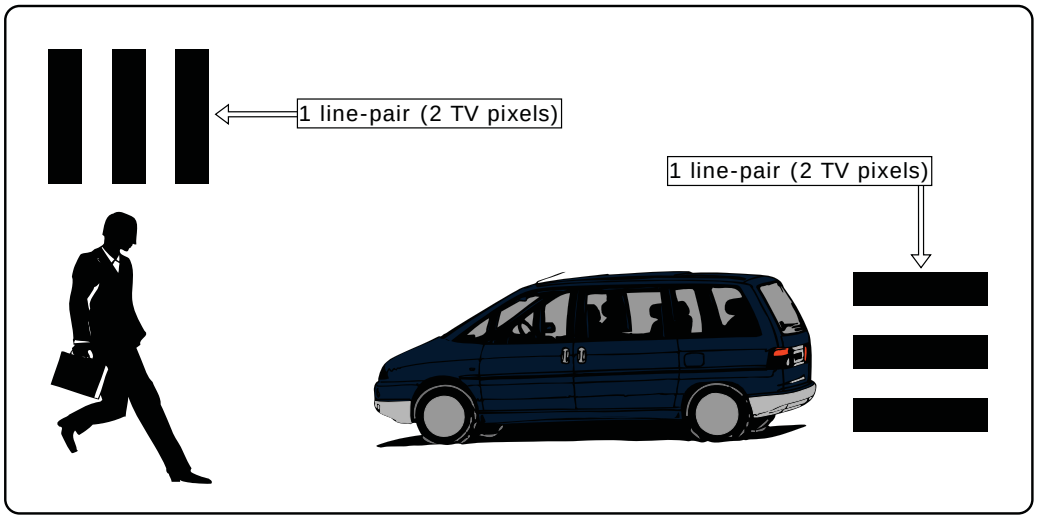


Figure III-G-1 - Examples of Critical Dimensions

b. Intelligent Video

Intelligent video originated with motion detection circuits which detected changes in the characteristic of the video signal in a defined area of the screen, known as a window. An operator could then be alerted to an event as it happened, greatly reducing the need for operators to stare at video monitors for long periods of time. The effectiveness of this technology has improved, especially in digital systems where software has been developed to cope with shadowing, blowing trees, and other environmental effects which created false positive alerts in early systems.

Digital video systems are now able to detect multiple objects in a scene (and exclude areas of the scene), track objects as they move across the scene, generate position coordinates for these objects as they move as well as speed data, and in some cases distinguish types of targets by class – a field known as pattern recognition, where the technology is progressing rapidly.

For most systems, these intelligent video functions apply to cameras which are not moving. That is changing. Object detection and tracking can now be done across multiple cameras and even as these cameras are panned and tilted, with the object data handed off and object track integrity maintained as objects move from the field of view of one camera to other cameras along the track.

Intelligent video is also able to analyze an object and make a determination if it is possible threat, based on "rules" established by airport security. A basic application of this is the monitoring of passenger traffic in a jetway - if persons exiting an aircraft reverse course, the camera monitoring that jetway will see the change in course and the object tracking software can "decide" to notify an operator in the Security Operations Center. More sophisticated behavioral "rules" are under development and will appear on the market as digital CCTV equipment continues to improve.

Intelligent video can also "associate" behavior or events, including events detected by other sensors such as infrared (thermal) imaging cameras and ground surveillance radars, to further aid security operations.

Within DHS, HSARPA is pursuing a research project, known as the Automated Scene Understanding Program (ASUP), to develop intelligent surveillance systems capable of correlating and interpreting fragments of information derived from video, radar, seismic, acoustic and other monitoring technologies.

The intent is to reduce thousands of objects, tracks, events, situations, behaviors and scenarios to the few that matter — so that security teams can respond before an attack occurs.

The key to "fusing" these sensor inputs is 3D visualization, in which a facility is diagrammatically shown in 3D on a monitor alongside a live image of a scene such as a jetway, ramp area, or facility access gate. The 3D image is able to zoom globally, from a virtual point above the airport to a specific access gate, based on information from access control devices or radio frequency tags (known as RFID). Persons or devices, including baggage, which have RFID tags can be tracked across an airport using wireless networks and located precisely at all times.

All of these features and advanced capabilities come at a price. Airports need to carefully weigh the benefits and costs, especially with regard to how these features and capabilities are to be implemented and the downstream support requirements.

A program which is to be implemented entirely in software may have a cost advantage, depending on software licensing rates, but it may also impact hardware by requiring more powerful CPUs and increased hard drive capacity, or reduction in the number of video cameras which a server can support simultaneously.

A program which is to be implemented as a new hardware appliance may impact available equipment space, electrical power, and network interfacing, in addition to requiring maintenance of the new equipment.

These types of issues should be considered in evaluating new system features and capabilities. 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 requirements as:

- detect and track at least one attempted intrusion in the of the perimeter fence segments simultaneously, and
- maintain tracks and generate horizontal position coordinates for intruders as they move inside the airport property, and
- superimpose the intruder tracks on maps and/or drawings of the airport and its facilities at operator monitors in the SOC, and
- Demonstrate 3D visualization of the events, in real time, on the operator monitors.

Airport security is faced with rapidly changing technology and rapid changes in the cost of deploying this technology. Both present challenges, and emphasize the need for properly engineering the security infrastructure so that new capabilities can be adopted as they become cost-effective.

c. Cameras

The type of detector used in a surveillance camera should be matched to the operational requirements. Some applications require low-light sensitivity, some will require small size to fit within dome housings, and some will require large detector arrays to be effective with long focal length optics.

Twenty years ago, the detectors in most surveillance cameras were based on the classical vidicon tube. Modern surveillance cameras use solid-state detectors, primarily charge-coupled devices (CCDs) 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 offers a higher pixel density, a broader dynamic light range, uses less power and is potentially less expensive because it can be fabricated with common computer technology.

Camera performance is a function of scene illumination and how a camera is positioned and mounted to view the scene. Scene illumination is especially critical at low light levels. Many designers assume that the ambient light in an area represents the light that is sensed by the camera. Cameras also sense reflective light, and the amount of reflected light depends on reflectivity of the surroundings. Dark areas, such as asphalt parking lots, have reflectivities as low as 0.05 (5 percent). If the ambient light at the darkest point

in a parking lot is .01 foot candle (fc), for a reflectivity of 0.05 a camera will sense only 0005 fc of the reflected light. Effective night operations are critical for airport security, and the surveillance cameras must be specified based on a realistic understanding of the actual environment.

For very low-light conditions, CCDs and CMOS arrays can be fitted with image intensifier modules to operate down to starlight scene illumination levels, but at significantly higher cost to acquire. Intensifier modules also increase operating cost because their reliability is less than un-intensified cameras. Adding supplemental lighting to permit the use of normal CCD/CMOS cameras should be considered as a cost-effective alternative to using intensified cameras.

For situations where no light is available, or where an alternative detection mode is desirable, cameras are available which operate in the 3 to 5 micron and 8 to 12 micron infrared bands. These cameras sense thermal energy and are commonly called thermal imagers. Because they operate at wavelengths longer than the wavelength of visible light, the resolution of infrared cameras is proportionately less than the resolution of CCD/CMOS imagers.

The common sizes of CCD/CMOS arrays used in surveillance cameras are shown in *Figure III-G-2* below. 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 proportionate to yield, and this favors the smaller array sizes. As a result, most surveillance cameras use 1/4-in and 1/3-in arrays, especially dome cameras.

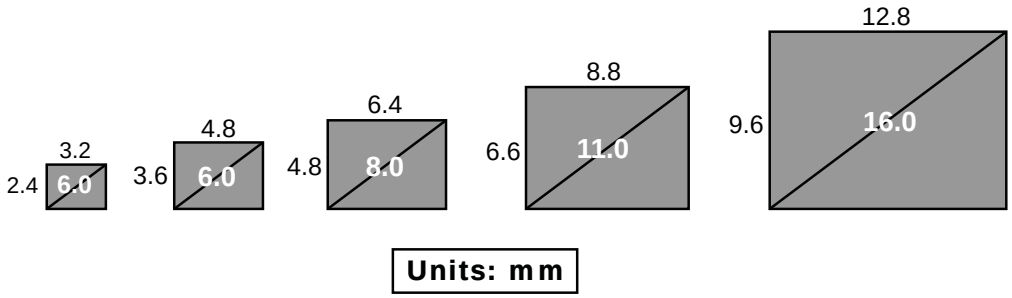


Figure III-G-2 - Dimensions of CCTV Detector Arrays

Detector size and the horizontal dimension of the detector in particular, plus the focal length of the camera's objective lens will determine the surveillance field coverage of a camera. The proper combination of detector size and focal length 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 be most important, especially for area coverage. In other cases, the ability to resolve target details will set the requirement. Camera and lens selection can also be constrained by factors such as space availability.

Magnification is a popular specification for camera lenses, but it is not a substitute for a definition of the operational requirements which should determine the needed coverage and magnification. The best assurance of having the proper camera and lens combination and realizing the expected performance is to test units under actual operating conditions.

In the case of 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" about the target being focused on the detector. Increasing the apparent magnification electronically, however, simply increases the size of the pixels. It adds no new "information" about the target and is not a substitute for a proper optical zoom range.

Since the purpose of surveillance cameras is to monitor intruders, using the Johnson criteria above, it should be possible to calculate the required camera-lens combination for the image quality needed at the distances and for the areas of coverage associated with each planned installation.

Video surveillance cameras should be sited for overlapping coverage to the extent practicable, as protection against any camera failing and also to provide alternate views of detected objects to enhance their detection and tracking. The extent of overlapping coverage should be shown in diagrams.

Table III-G-2 below shows how horizontal angular and linear field coverages vary with detector size for a sampling of objective lens focal lengths. Coverages are a function of detector width and lens focal length

Table III-G-2 - Horizontal Angular and Linear Field Coverages 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	35.5	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	4.9	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 Coverage at 1000 ft (ft)				
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

For airport operations, the parameters of a CCD/CMOS camera which are operationally significant 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 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 likely to occur, airport security in establishing its 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 (FSR) 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 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.

d. Interior

In most cases, a camera can be used within a facility as well as outdoors, the difference being the type of housing required for the particular environment. Consideration should be given to using the same cameras indoors and outdoors to simplify 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 unnecessary. 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.

e. Exterior

Outdoor cameras will be subject to local temperature, wind, rain and snow. They may also be installed on poles or sides of buildings were access is limited or difficult. Cameras which 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.

f. Lenses

Camera lens types can be classified as:

1) Fixed focal length lenses: The lens is manufactured to a specified focal length selected for the particular application.

2) 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 the coverage to the scene to be monitored.

3) Zoom lenses: A zoom lens is a varifocal type in which the zoom function is motorized so that it can be controlled remotely by an operator in the Security Operations Center (SOC).

For airport security operations, the parameters of a lens which are operationally significant include:

- Focal length: This parameter, expressed in millimeters (mm), will determine the angular field of view, in degrees, and linear field coverage, in feet or meters, as well as the viewing magnification.
- Relative aperture: Also known as the f/#, this parameter is the ratio of the lens focal length to the diameter of its clear aperture. It is a measure of the ability of a lens to capture light, and is especially important for viewing under overcast or low-light conditions. Doubling the numerical aperture, from f/2 to f/4, will halve the amount of light transmitted by the lens to the camera detector and that can easily impact camera performance.
- For zoom lenses, the relative aperture is normally stated at the minimum focal length setting, e.g., f/1.4 at 25 mm, and as the focal length 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. It will also decrease the light gathering ability of a lens so that a lens which performs effectively at a focal length of 25 mm may not perform well at a higher numerical aperture under the same scene illumination. This factor should be considered in selecting zoom lenses.
- Iris range and control: An iris is an internal diaphragm used to control the transmission of light through a lens. The iris range, normally expressed as in relative aperture terms, e.g., f/1.4 to f/400, is important for areas subject to intense sunlight or strong supplemental lighting. Motorized lenses normally provide for an iris to be controlled automatically based on the level of scene illumination.

g. Video Standards

The resolution and frame rates for U.S. and European video standards streams are shown in *Table III-G-3* below.

Table III-G-3 - Horizontal and Vertical Resolution of U.S. and European Video Standards

		CCD/CMOS Array		Depth 256 Colors	Video Rate
Standard	Resolution	H Pixel	V Pixel	bits	frame/sec
USA	VGA	640	480	8	30
NTSC/	QCIF	176	112	8	30
RS170	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

h. Video Storage

Video storage, whether in analog (tape) or digital (hard drive or tape) formats, can present significant design, management, and cost challenges, especially for airports having several hundred or more video cameras.

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) if the video is transmitted over an IT network, the available network transmission bandwidth.

The output of analog video cameras, especially for legacy systems, will normally be transmitted to a video matrix switch, to be distributed to monitors and recording devices. If the video storage is done digitally,

either using digital video recorders (DVRs) or a networked storage array, then the conversion from analog to digital format and the compression of the digital stream will be done at the point of reception either within a DVR or similar device or using an external converter and server. The analog output of the cameras will not be changed.

If IP cameras are used, then 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 which 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 which reflect the limitations of the embedded electronics, for example, 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.

There are several different algorithms available for compressing video streams to minimize the required storage. The airport operator can also adopt various storage scenarios to further reduce the amount of storage required. These scenarios can include varying the resolution of the stored images, or varying the video frame rate, or storing only images which in which motion events have been identified.

Table III-G-4 on page 171 illustrates the storage capacity that would be required for several storage options at airports operating 100 and 500 video surveillance cameras. The table assumes that the incoming video streams are compressed using algorithms such as MPEG4 and MJPEG2000 with 30 days of storage required and U.S. NTSC/RS-170 video. In *Table III-G-4*, a 30 day period for storage is used as a baseline because it is a common expression of airport operators when the design process begins.

Given the variations in compression algorithms and how they are implemented, as well as their constant updatings, the capacity numbers should be considered illustrative rather than absolute. The relationships of the storage options, however, provide guidance for airport security designers in selecting an appropriate storage strategy compatible with budgets and operational requirements.

Table III-G-4 - Examples of Digital Video Storage Options

	Resolution, Storage Period, and Frame Rate Options	Camera Resolution		Required Storage in Terabytes (TB)	
		H Pixel	V Pixel	100 Cameras	500 Cameras
1	All images @ 30 fps				
1a	4CIF - 30 days storage	704	480	159	797
1b	CIF - 30 days storage	352	240	40	199
2	Motion-event images only @ 30 fps				
2a	4CIF - 30 days storage	704	480	24	122
2b	CIF - 30 days storage	352	240	6	30
3	Hybrid Storage Strategy @ 30 fps				
	4CIF - all images stored for 3 days, plus	704	480	16	83
	4CIF - motion-event images stored for 27 days	704	480	22	110
	Total			38	193
4	Hybrid Storage Strategy, variable frame rate				
	4CIF - all images stored for 3 days @ 30 fps	704	480	16	83
	4CIF - motion-event images stored for 7 days @ 30 fps	704	480	6	29
	4CIF - motion-event images stored for 20 days @ 5 fps	704	480	3	14
	Total			25	126

Option 1 shows the amount of hard disk or tape storage that would be required for high resolution, full-screen images (4CIF) and for quarter-screen images (CIF) if all images are to be stored.

Option 2 takes the numbers from Option 1 and eliminates those images which are not tagged as having motion in the scene. The amount of motion content will vary from camera to camera by location and by time of day. An average of 15 percent motion content is used in Option 2 but each airport camera application has to be considered individually be the video system designer.

Option 3 still calls for storing only motion-event imagery, but at full resolution for the nominal 30 day period. In many applications, reducing image resolution to quarter-screen will not be possible, especially if the imagery may be used to identify persons for law enforcement purposes.

Option 4 is similar to Option 3 with the exception that the frame rate after day 1o has been reduced to 5 fps, which is satisfactory for many archival security requirements.

The resulting savings is hard disk cost, equipment rack space and electrical power, and equipment maintenance which can result from hybrid storage strategies suggest that scenarios of this type, tuned for the airport's particular needs, should be investigated by airport operators before specifications for video storage are established for design purposes.

i. Retrieval and Distribution

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 has 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 is 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 by the airport IT department. This may require that such transfers be encrypted using a U.S. Government approved technique such as the Advanced Encryption Standard (AES) developed by the National Institutes of Standards & Technology (NIST).

Video image distribution within government agencies and with non-governmental agencies may involved Security Sensitive Information (SSI), which is controlled by 49 CFR 1520 governs the maintenance, safeguarding, and disclosure of records and information that TSA has determined to be Sensitive Security Information (SSI). SSI is sensitive but unclassified information related to transportation security that is provided to entities in the transportation sector on a need-to-know basis in order to carry out their security obligations. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as protected critical infrastructure information (PCII) under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

j. Video as Evidence

There are several issues which should be considered in specifying evidentiary-quality video surveillance.

- Airport security normally does not require "identification" quality video imagery, in contrast to law enforcement which needs to identify persons for prosecution.
- As the Johnson criteria above show, "identification" quality video requires several times more "information" to provide detection, orientation, or recognition. This additional "information" translates into more capable, and more costly, video surveillance cameras, lenses, and storage devices.
- An operational analysis should be performed to determine those specific locations where "identification" quality video imagery will be required.
- Video editing should be strictly controlled, by defined procedures, and be done only be persons having a valid need-to-know. These individuals should be trained to deal with law enforcement agencies and to work with these agencies to define what means of authentication the courts are likely to require. If and when the courts establish standards for authenticating digital imagery, airports will have to respond in order to maintain the integrity of the process.
- Airport personnel who participate in this process should also be briefed so that they understand what will be expected of them in court regarding the integrity of digital video records when evidence is presented.

3. System Design and Infrastructure

Historically, video surveillance systems have been designed as components of a broader facility security system or as stand-alone systems. That is changing as information system/ information technology (IS/IT) networks become more capable, video security systems become "digital" and also "smarter", and multiple users in the security community want to be able to monitor an event in real time from different locations over the Internet or over wireless networks.

The result is that video surveillance systems are increasingly being integrated with an airport's IS/IT network, with video camera outputs traveling over the IS/IT infrastructure rather than over a dedicated security infrastructure. This trend toward networked video surveillance will grow as the underlying digital technology continues to improve.

In a typical IS/IT network, video camera outputs are either digitized and compressed at the camera heads or are transmitted using fiber optic converters to a network device which digitizes and compresses the signals. The

digital data streams can then transmitted over the network infrastructure, assuming adequate transmission bandwidth exists for the number of cameras involved.

a. Networks

Traditionally, video systems have been configured with analog video cameras home-runned [Please explain "home-runned"] over coax or fiber cabling to matrix switches [please explain "matrix switches"] located in the airport Security Operations Center (SOC). Storage has used video tape recorders, recently replaced by Digital Video Recorders (DVRs). DVRs provide on-demand access and eliminate the problems of managing tape archives.

The advent of high-speed fiber-based digital information system (IS/IT) networks, digital video compression technology, and low-cost digital storage means that airports can now afford to network video surveillance systems.

By networking video cameras, the images from any camera can be viewed by any monitor on the network, in real time, as well by monitors off-site that have broadband access to the Internet and have the necessary security permissions.

In the networked video model, airport security shares the transmission medium with other network users. In addition to bandwidth demands and quality of service issues, this arrangement also raises issues of equipment selection (and cost, for which airport security may be the funding source), data security, and network reliability. The airport IS/IT department is likely to have primary responsibility for all of these matters.

Standards are essential for networks to function properly. There are three main networking standards bodies that should be of interest to airports:

- In the U.S., 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 U.S., the Internet Engineering Task Force (IETF) publishes standards for protocols and devices which operate over the Internet.
- In Europe, the main standards bodies are the International Telecommunications Union (ITU) and the International Organization for Standardization (ISO).

The transmission distances permitted over networks cabling varies by type of cable. The applicable IEEE performance standards for Gigabit Ethernet networks are listed in *Table III-G-5* on page 174.

Table III-G-5 - IEEE Ethernet Standards and Cable Distances for Gigabit Service

Network Technology	IEEE Standard	Cable Type and Bandwidth		Total Distance
1000base-sx (850 nm short wavelength)	802.3z	62.5-micron multimode fiber	160 modal-bandwidth (MHz*km)	2 - 220m
			200 modal-bandwidth (MHz*km)	2 - 275m
		50-micron multimode fiber	400 modal-bandwidth (MHz*km)	2 - 500m
			500 modal-bandwidth (MHz*km)	2 - 550m
1000base-lx (1300 nm long wavelength)	802.3z	10-micron single-mode fiber (plus same as 1000Base-SX above)		2 - 5km
1000base-cx	802.3z	Twinax copper		25m
1000base-t	802.3ab	Cat5, Cat5E, Cat6 UTP copper		100m

Network standards continue to evolve. The IEEE has approved standards for 10 Gigabit Ethernet transmissions over both copper and fiber, which will provide airports with even greater opportunities for networking surveillance video.

Given the frequency of moves/adds/changes (M/A/C) at airports, it is important that all video networking be configured, installed, and tested according to recognized standards.

The network infrastructure should also support mobile access to video imagery. Airport security personnel are frequently not in the Security Operations Center (SOC) when an event happens. Being able to see what is happening on a portable digital assistant (PDA) - and having two-way voice communications to the personnel at the location – is operationally desirable. At this time, two makes of PDAs can provide this functionality – the iPAQ series by Hewlett Packard and the Axion series by Dell – provided the airport has installed Wi-Fi wireless coverage in its terminals, holdrooms, ramp areas and other facilities, and provided the video management software has Internet connectivity and also incorporates two-way voice capability.

b. Cabling

Since CCTV became a fixture at airports, video cameras have been home-runned to a Security Operations Center (SOC) over dedicated copper cable, usually coax type, or over fiber optic cable. The selection of cabling has usually been 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).

The video cables are then terminated in multiplexers or in matrix switches, from which the signals are routed in analog form to monitors and to storage devices such as tape recorders and digital video recorders (DVRs).

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 home-running the cameras to a central point.

Network copper cabling can be Category 5/5e and 6 unshielded twisted pair (UTP) or Category 7 shielded twisted pair types. Network fiber cabling can be multimode or singlemode types.

In the U.S., the Telecommunications Industry Association (TIA) generally is the lead body for cabling standards but it often publishes jointly with the Electronic Industry Alliance (EIA) and the American National Standards Institute (ANSI).

A "Standard" defines a method of connecting all types of vendors' voice, video, and data equipment over a cabling system that uses a common medium, common connectors and a common topology. This means that an airport building can be cabled for all its communications needs without the planner or architect having to be concerned about what type of equipment will be used.

c. Wireless Systems

The three types of wireless systems that are likely to be useful for airport security are:

- Radio frequencies which are licensed to the airport by the Federal Communications Commission (FCC).
- Radio frequencies which 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 which 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.

The alternative to using the Wifi bands, obtaining a radio frequency 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 if properly prepared, but obtaining a license is never guaranteed.

For this reason, the FCC has set aside several frequency bands for unlicensed operations. The most popular commercial bands are the so-called Wi-Fi frequencies developed for wireless local area networks (WLANs) described in *Table III-G-6* below.

Table III-G-6 - Unlicensed Wireless Network Spectrum Assignments

Radio Band (frequencies)	Description and Application
902.00 to 928.00 MHz	FCC Part 15 Subpart C, also known as the ISM band.
1.910 to 1.920 GHz 1.920 to 1.930 GHz	FCC Part 15 Subpart D - asynchronous FCC Part 15 Subpart D - isochronous
2.400 to 2.483 GHz	IEEE 802.11 b/g Wireless LAN, also known as Wi-Fi. The "b" standard specifies a maximum data transfer rate of 11 Mbps and an operating frequency of 2.4GHz. The "g" standard specifies a maximum data transfer rate of 54 Mbps and an operating frequency of 2.4GHz. IEEE 802.15 Bluetooth also uses this band
5.150 to 5.350 GHz 5.250 to 5.350 GHz 5.750 to 5.875 GHz	IEEE 802.11a Wireless LAN, also known as Wi-Fi. The "a" standard specifies a maximum data transfer rate of 54 Mbps and an operating frequency of 5GHz.

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.

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 which must be delivered should not use the Wi-Fi bands, however, if an airport and its tenants can agree to reserve the 802.11 a band solely for airport use this problem can be mitigated.

Issues of Wi-Fi interference and transmission security will require close cooperation between airport security and the airport IS/IT department.

Many airports already have 802.11 wireless local area networks (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 re-affirming that it alone can regulate radio operations.

Airports 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.

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 environmental conditions of concern before a commitment is made to such equipment.

d. Choice of Equipment

Surveillance cameras, or sensors, can generally be classified as operating (a) in the visible band, using light reflected by the target, or (b) in the infrared bands, using thermal energy emitted by the target. The relationships of these bands to each other and to other bands of the electromagnetic spectrum are shown in *Figure III-G-3* below.

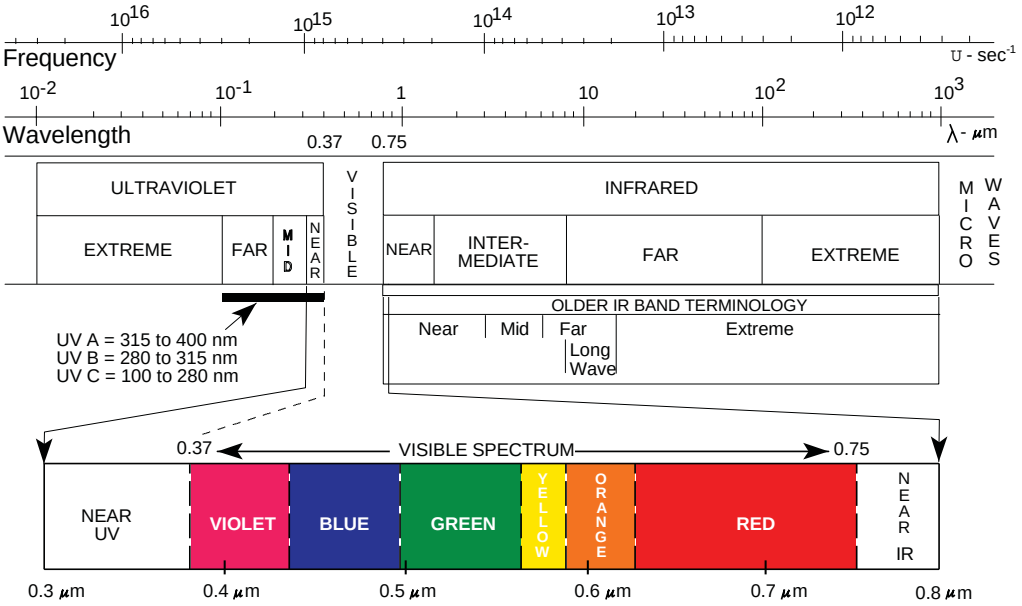


Figure III-G-3 - The Electromagnetic Spectrum

Surveillance cameras operating in the visible band are often specified in technical terms, e.g., resolution or pixel count. These specifications are useful to airport personnel only when related to operational requirements, such as target detection and identification. There is a considerable difference in the amount of "information" that a system must present to perform these functions.

Visual surveillance begins with an understanding of (a) what "surveillance" means for the airport applications to be addressed, and (b) the technical and equipment options which can meet these requirements.

e. Lighting & Special Operational Conditions

Whether lighting is exterior or interior, the placement and amount of lighting must address basic issues such as point light sources in the field of view (including streetlights and vehicle headlights at night), reflections from metallic and glass surfaces at various times of day and various sun angles, and the sensitivity of camera-lens combinations. Terminals with large glass facades, for example, may at some time in 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 under such circumstances.

Supplemental lighting may be needed for video cameras to function properly in areas such as a fenced perimeter which 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 (IR) illuminators, which cannot be seen by the naked eye but which can be sensed by a CCD/CMOS array, can also be used when visible lighting is undesirable. IR illuminators located at video

cameras are generally limited to short distances because of the attenuation losses in illuminating the target and then 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. These factors should be studied and the system designer should provide calculations to support any proposed illumination plan.

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 1.0 ft-candles of luminance for sidewalls and footpaths with a uniformity ratio not greater than 4:1 for parking facilities. Lighting should be elevated to 30 ft 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, but metal halide lamps are also more costly. Another option, which is becoming increasingly attractive, is the use of light emitting diodes (LEDs). These solid-state devices are smaller and use much less power than conventional lamps, but they have been limited in power output and, until recently, have not been available in white color.

The lighting industry has set a goal for white LEDs of reaching an output of 150 lumens per watt (lm/W) by the year 2012. This research and development is being supported by the U.S. Department of Energy as part of its Building Technologies Program. In 2004, white LEDs were able to demonstrate outputs of 80 lm/W, which is comparable to existing compact fluorescent and incandescent lamps. As LED components continue to improve in efficiency, LEDs will become increasingly more attractive for area illumination.

It is advisable for airport personnel to survey lighting in areas to be secured by video cameras using a light meter to measure illumination levels, both existing and proposed. The ability of video cameras to function properly under these conditions should then be tested.

Section III-G Surveillance and Video Detection Systems Checklist:

- ☐ **Establish Operational Requirements**
  - Review surveillance needed at each site
  - Camera Placement and Mounting
    - Security
    - Access for Maintenance
    - Appearance and Aesthetic Issues
  - Field coverage
    - Fixed
    - Variable (pan/tilt mounts)
  - Camera Resolution and Lens Focal Length (magnification) required for
    - Detection
    - Classification
    - Identification
    - Recognition, including law enforcement requirements
  - Intelligent Video Functions – to enhance video performance and reduce personnel
    - Target Tracking
    - Discarded/Abandoned Object Detection
    - Software-based rather than dedicated appliances
  - Special Coverage of Security Checkpoints
  - Lighting
    - Exterior Perimeter
    - Interior Areas
    - Infrared (non-visible) Lighting
  - Video Storage
    - Duration
    - Resolution
    - Frame Rate
- ☐ **System Design and Equipment Selection**

- Balance operational requirements, functionality, cost, and security
- Information Retrieval and Distribution
  - Privacy
  - Statutory Constraints
- Reduce security force and police response requirements
- Power/Data – power outlets for each video camera
  - Power from emergency operating conditions
  - Battery backup not required
- Camera Selection and Interfaces
  - Type – analog or IP, color or monochrome – or a mix
  - High-light (bright spot) and low-light lever performance
  - Infrared (thermal) Imagers – for special areas
  - Link CCTV to ACAMS alarm signals
  - Pan/tilt/zoom camera mounts – used to minimize camera quantities, provide redundant coverage, reduce personnel required for monitoring
  - Mount cameras in locations with accessible ceilings/cabling route
- Video Storage
  - Architecture and Storage Strategy
  - Hard Drive Capacity
  - Local and network storage
  - Scalability
  - Management
  - Emergency Backup
- Networked Video Cameras
  - Network Architecture – design to minimize bandwidth required
  - Browser User Interface
  - Storage Network Interfacing
  - Network Security
- Displays and Security Operations Center
  - Ergonomics – design for extended and emergency operations
  - Integrated video feeds to minimize display quantities
- Remote (off-site) Video Access
  - Browser User Interface
  - Secure Access
- Camera Installations – derived from operational analysis of surveillance required
  - Ticket Counters
  - Kiosks
  - Terminal Apron
  - Security Checkpoint Areas
  - Public Lobby Areas
  - Roadway/Curbside Baggage Areas
  - Loading Dock/Police Parking Areas
  - Administrative and Tenant Areas
  - Airside Access Doors and Gates
  - Baggage Handling and Claim Areas
  - FIS Areas
  - ACAMS Access Points
  - Runways and Taxiways and Airfield
  - Cargo/GA/FBO Ramps
- Public and Employee Parking Areas

☐ **Procedures and Personnel**

- User-Friendly Design
- Maximum 4 Monitors per Operator
- Training Plan
- Emergency Operations Plan
- Emergency Maintenance Plan
- Planned Maintenance/Outage Plan
- Equipment Service Tracking
- Periodic Upgrade/Evaluation

Section H - Power, Communications & Cabling Infrastructure Systems

Although power, communications and cabling infrastructure systems are seldom seen by airport patrons and employees, their design and efficiency are critical to the operation and security of the airport. These systems are fundamental to both airport operations and airport security. Loss of functionality or data integrity on these systems jeopardizes the airport's safety and security. Efficient and secure design is critical for these systems.

The combination and interconnection of these systems throughout the site is cumulatively referred to as the Information Technology (IT) infrastructure and sometimes as the "Premises Distribution System." Component portions should be designed and installed to operate seamlessly. If any one or combination should malfunction, the security of the facility can no longer be assured. Thus, the design process for an integrated cable and infrastructure system should examine each of these elements at the earliest possible stages of design, and should examine them both internally within the system itself, and externally at every point where they connect with security or other systems, to assure compatibility, connectivity and security throughout. The equipment and components of the individual power, communications and infrastructure systems also should be designed, chosen and placed in locations that secure them and provide for reliable operation during an emergency.

While some of the most critical data being transmitted pertains to the airport's access control and monitoring system (ACAMS), 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 cause delay of flights or threaten public safety.

The best way to secure data or systems is by limiting access through secure IT infrastructure systems design, and continued operational and maintenance supervision.

1. 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 (EDS) and other screening and security equipment.

In providing redundancy or back-up, the designer should consider such things as the location and capacity of stand-by 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 when possible) and spatial/geographical separation where multiple feeds exist (particularly regarding singular vulnerability at the actual point of service) are desirable capabilities to minimize loss of power and consequently airport function.

Consideration should be given to the fact that a majority of the airports nationwide are not new facilities. Most of these facilities were built prior to introduction of contemporary integrated systems; the electric power distribution infrastructure typically is not configured to meet current security requirements.

A minimum of two power distributions (busses) should be considered, one for mission critical systems and one for non-critical usage. The primary goal of electrical system design should be protect the safety of personnel within the facility and enable their 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 (buss) distribution system. Use of automatic transfer switches (ATS) 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 main-tie-main arrangements, uninterruptible power systems (UPS) and battery backup systems.

UPS power should be utilized in each Main Distribution Facility (MDF) and Intermediate Distribution Facility (IDF) room, and should have a designed capacity for at least 25% future growth. Coupled with the use of line-powered CCTV, an access control loss of power need not violate the integrity of the terminal security system.

Backup power for lighting is required for life safety systems; many options that are allowed under local building codes provoke considerations in reference to security

- Generators are (the most common form of emergency backup; however, most local building codes require generators to come on-line 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 and 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 (HID)-type light fixtures that provide lighting for larger areas.
- The required egress lighting level is one foot candle (fc) in the path of egress. Most cameras will record down to 0.5 fc; 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 system.

Integration of the security system with life safety systems is critical. Both the Uniform Building Code (UBC) and the International Building Code (IBC) 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 authority having jurisdiction is critical to designing in conformity with this requirement 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 fire alarm activation as a diversion, which could enable access to restricted areas and/or the aircraft operations area (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.

2. Communications Infrastructure

The cable infrastructure, including the hardware and electronic components supporting voice and data transport of security, IT, and related systems, is referred to as the "Premises Distribution System" (PDS). The PDS is composed of two elements: the passive infrastructure, and the active equipment/software. The passive element includes the fiber optic and metallic conductors that provide physical connectivity throughout the airport.

a. 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 provisioned over the active infrastructure including Ethernet, Token Ring, ATM, Frame Relay, and others. The implemented networking technology determines which data transmission methods can be implemented 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 Internet Protocol or VOIP), Electronic Visual Information Display Systems (EVIDS), Common Use Passenger Processing Systems (CUPPS), public address systems, building management systems, closed circuit television systems (CCTV), access control and alarm monitoring systems (ACAMS), etc. Using this approach, airports are able to achieve economies of scale to implement communications infrastructures that provide a level of fault tolerance and resiliency at much lower overall costs than if the individual systems were implemented as stand-alone infrastructures. With technological advancements that have occurred within the past five years, security strategies for isolating an individual system's data can be implemented that provide for a more secure network than if a stand-alone system were used.

b. 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 repair times alone warrant careful consideration of these issues.

If security and data transmission medium (fiber optic or cable) are of the same quality and contain spare capacity, each may provide an alternate route for mission critical applications of the other. 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 typically accomplished by placing security related cabling in conduit and limiting access to communications rooms, where security related cabling terminates.

Passive infrastructure should be designed in accordance with 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 tray 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. Wire-tapping is also a possibility in conduits as pull-boxes and access points are required for this system as well.

c. Active Infrastructure Component

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 provisioned by active infrastructures. As a result, the demand for bandwidth and guaranteed quality of service 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 communications rooms located throughout the airport campus. The physical connectivity between components within each closet and between closets is achieved through the passive infrastructure.

When designing an active infrastructure to support security related systems two primary elements should be considered: reliability and security. The design or evaluation of a shared bandwidth network should include fault tolerance with a minimum of 99.999% uptime. This can be achieved using meshed topologies that provide redundant routes between networking components, dual power supplies and dual supervisor modules (as applicable) for individual components, uninterruptible power supplies (UPS), and the implementation of Quality of Service (QoS) techniques.

d. Telecommunication (TC) Rooms

It is beneficial to design all telecommunication (telecom) rooms, termination closets, wire rooms, and other components of the passive infrastructure in as short and direct a line as possible to each other, to minimize cable run length. In multi-level 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, as, for example, if a fire in an upper level telecom room

leads to water damage on floors below. In any case, communications rooms must be established to support the BICSI and ANSI/TIA/EIA–568B requirements that no end device is located more than a ninety 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 should provide 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 as appropriate.

Special consideration should be given to providing adequate clearances and space for access to the equipment, HVAC equipment to support typical heat loads generated by communications equipment, and local UPS to power equipment in the event of a power failure. 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. Access to these rooms should be controlled.

Telecom rooms that require tenant access should have a clearly defined tenant area. This could be in the form of a physical barrier providing separation, a rack configuration that limits accessibility, locking co-location cabinets that provide locking mechanisms for tenants as well as owner cabinets, or other appropriate measures.

e. 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 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.

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 FSD 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 doesn't immediately imply "security" 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:

- Use 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; they are typically above a dropped ceiling within a plenum space. Sometimes roof mounted raceways and cable trays are used to accomplish connectivity.
- 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 cabling cutting by installers and maintainers of adjacent systems.

The 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 protection but can cause installation and/or maintenance errors.

f. Cabling Infrastructure Systems & 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 and isolating cabling and its surroundings and/or other 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 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 sued on a first-come-first-served basis in the absence of centralized, thoughtful management and control.

3. Security of Airport Networks

As most airports move toward combining administrative, communication (radio, phone, data), information display (flight, baggage, paging), mechanical (HVAC, baggage systems, environmental controls, fire systems) security and other systems onto one overall network, the concern for network and information security increases. Issues related to network security, availability, and access are discussed below:

a. Network Availability

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 may be considered to interconnect mission-critical computing equipment and platforms. The dual network cables could be routed along physically diverse paths to minimize the chances of being damaged at the same time.
- 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 fire, explosion or other event.
- The use of Power Distribution Units (PDUs), alternate sources of power from different substations, and other redundancies helps to mitigate power outage problems. (Note that 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.)
- A UPS should be installed at each Intermediate Distribution Facility (IDF) and Main Distribution Facility (MDF) to provide both reliable power and clean power to the downstream loads.
- 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. (Note that the use of K-rated transformers does nothing to correct the harmonics on an electrical system, it merely generates more heat that has to be dealt with in the HVAC system.)
- Systems such as 400-hz aircraft ground power units and chargers for electric ground service equipment should be isolated and fed from dedicated switchboards if possible.

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 when needed.

Network architecture should include the appropriate "meshed" configuration to provide multiple routes between network components in the event of equipment or cabling failures.

b. Network Security

The security of data, communications and information systems at an airport can be critical to an airport's operation and safety. While certainly some of the most critical data is that pertaining to the electronic security system, the security of other data and systems such as flight information, lighting and cooling systems, and radio communications systems can also determine if an airport is open or closed. Access to virtually any data or systems within an airport, when in an unauthorized individual's possession, could at a minimum cause the delay of flights or inconvenience to the public.

Communication and data networks should be secured from unauthorized access. Unauthorized access can take many forms:

- Authorized individuals failing to log off or re-secure their access points or computers, making available undetectable unauthorized access
- Authorized individuals gaining access to portions of the network they are not authorized to access
- Unauthorized individuals gaining access to the network from computers or systems that normally allow access to authorized individuals, either by "hacking" or by using an authorized individual's passwords or access codes
- Unauthorized individuals gaining access to the network from computers or systems on premises that normally do not allow access
- Unauthorized individuals gaining access to the network through external connections such as modems or wire-taps

c. Network Accessibility

Wide-Area Network (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 and airport organizations.

d. Information Storage Availability

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, providing information access. To ensure high availability storage systems, airport design should take into account storage redundancy and back up. Storage redundancy may be achieved by mirroring storage devices in different locations via local area networks, using Random Array of Inexpensive Disks (RAID) techniques, Storage Area Network (SAN) techniques, Network Attached Storage (NAS) techniques, or others. These strategies require the airport to allocate separate facilities for redundant storage system equipment. The distance between storage system rooms should be great enough to reduce the chances of all the rooms being damaged at once due to, for example, explosion or fire.

4. 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 foreseeable future, it may be prudent to include sufficient

conduit, pull strings, cable or fiber, terminations, shielding or other rough-in elements to those locations in an earlier construction job. This helps avoid future needs to tear up and repair walls or floors, dig trenches, and pull cable.

5. Telecom Rooms

Due to the distance limitations on certain secondary wiring technologies, specifically Cat5 cabling, secondary telecom rooms should be distributed throughout the terminal to provide adequate coverage for both planned and future applications

Working space for maintenance personnel should be provided, and there should be enough room to accommodate reasonably foreseeable 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 as appropriate.

Special consideration should be given to providing adequate clearance to access the equipment, HVAC (some equipment is quite heat generating) and local UPS to power equipment in the event of a power failure. At one designated main telecom room, space should be allocated for infrastructure operating staff and system administrators to work, and a small maintenance and spares storage area should be considered. These rooms should have controlled access, preferably automated.

It may be appropriate to consider HVAC system backup. Most terminals are fed from a central electrical plant of some kind, either remotely or on-site. Although electrical HVAC equipment may be powered by an emergency generator, the chilled water system may not, which negates the effectiveness of the electrical components in the cooling system. Sensitive electronic equipment in a non-air-conditioned room likely will shutdown in a short time due to overheating. Dedicated terminal units backed up by an alternate power source should be considered for critical equipment rooms, and should be sized with future growth and higher equipment densities in mind.

Telecom rooms that require tenant access should have a clearly defined tenant area: potentially separated from the airport-controlled area by a physical barrier, or appropriate rack arrangement.

Raised floors for either IDF or MDF locations allow for below floor cable management systems and under-floor air distribution to maximize cooling of the rack-mounted equipment. A carefully designed and installed signal ground system is critically important to successful operation of digital data equipment.

6. Radio Frequency (RF)

There are three broad considerations when RF-based communications or devices are introduced to an airport environment:

- Is RF-based communication the most efficient and cost effective way to accomplish the necessary tasks?
- Will RF-based communication require infrastructure support that is 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 potions 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.

a. Environmental Considerations include:

1) Electromagnetic Environment

Potential sources of electromagnetic interference with RF communications include:

- Cell Phones
- Licensed and unlicensed equipment
- Metal detectors
- Portable devices such as pagers, computers)
- Power Generators
- Power lines

- Power transformers

2) Physical Environment

Physical environment can affect RF communications, depending primarily on the frequencies used by the system, and to a lesser extent on the communications protocol. Relevant environmental variables include:

- Dust and dirt
- Rain
- Snow
- Temperature
- Weather considerations

b. Regulations

Federal Communication Commission (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 for the Radio Frequency Interference Program. ASR-100 may be helpful in working though spectrum allocation issues associated with an RF telecommunications design at an airport. Key design decisions include antenna placement, cables and routing, and whether some functions might remain hard-wired.

c. 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/omni-directional considerations
- ATC communications interactions and interference
- Coverage areas (and dead spots)
- Mobile or Portable
- Obstructions
- Other collocated or local transmitters, including those external to the airport, which have the potential to "interact" with airport RF communications systems
- Robustness of Link
- Shielding
- Time criticality

d. Unlicensed Wireless LANs

Wireless LANs are permitted to operate without FCC licenses in the 2.4 and 5.8 GHz range. These LANs usually employ "spread spectrum" techniques for transmission, and are now found in airline VIP lounges as well as airport operational areas. Some wireless installations use "legacy" versions of LAN products, raising potential security concerns. Any security application and any application with security related data that proposes to use wireless LAN transmission should consider methods to protect sensitive data.

Wireless technology is convenient and often less expensive to deploy than wired data communication technology, but is has inherent risks. Any omni-directional transmission, including the majority of Wi-fi type systems, is at risk of a denial of services attack, even if the best possible security and encryption measures are deployed. For this reason, wireless transmission should not be used for critical transmissions whenever possible.

Point to point uni-directional 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 in all weather circumstance.

The 802.11b/g band, at 2.4GHz, is very popular and widely used by both individual travelers and by airports and their tenants. The popularity of this band raises the issue of self-jamming. The 802.11a band, at 5.8GHz, is not so widely used and also provides greater channel capacity than the 802.11b/g band. For these reasons, an airport should consider as a policy, encouraging tenants to utilize the 802.11b/g band and

reserving the 802.11a band for the exclusive use of the airport. Because these bands are controlled by the FCC, this will likely require language in the agreements with air carriers and other tenants to abide by this policy.

e. Considerations Related to the Use of Radio Frequency ID Devices for Security

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 air cargo. Standards for RFID tags are not yet mature at the time of this writing. One standard would use RF frequencies in the 13.56 MHz range; another in the 2.45Ghz range. It should be noted that this latter range is available for unlicensed use within the United States and is currently the frequency range of choice for a number of commercial wireless LANs already appearing in airline lounges and in use by some airlines for bag systems using 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 a RF spectrum survey of the airport, should be considered.

1) 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 and hence their radiation emission and susceptibility can be better predicted and controlled. Also, the 'outside of the physical building' RF environment is much more unpredictable and hence efforts should always be taken to 'isolate' as much as possible internal-to-the-building RF from external-to-the-building RF.

2) Choke Effects

At the lowest frequencies (such as generator resonance, etc.) wave lengths 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.

7. Information Assurance for Airport (Re) Construction

This section provides an outline of concerns regarding "Information Assurance," the process of detecting, reporting, and responding to cyber threats. These considerations include both design and procedural issues.

a. Threats

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 on 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.

8. Data Transport Vulnerabilities

This section pertains to data transport across the public switched telephone network (PSTN) and not to physical transport.

Most telecommunications in the United States today are handled using Common Channel Signaling (also known as "System 7"), and go through fiber optic cables. There is an illusion that this is a very secure means of transporting data; it is an illusion because:

- Fiber optic transmission protects only against RF eavesdroppers.
- System 7 is extremely vulnerable to software "bugs", such as a mistyped symbol in the SS7 protocol code.
- Most fiber optic lines use Synchronous Optical Network protocols (SONET) that are managed remotely through networks that use packet data, which, in turn, is usually uuencoded ASCII and hence vulnerable to intrusion and faked addresses.

Approaches to mitigate these issues include developing technical means to utilize this infrastructure securely despite its inherent vulnerabilities. This can be done through a combination of:

- Encrypting sensitive data prior to being shipped through SS7/Fiberoptics. This is the essence of well-designed VPNs.
- Path diversity (redundancy): Sensitive data should be shipped through multiple diverse paths.

Section III-H - Power, Communications & Cabling Infrastructure Systems Checklist:

☐ **Secure components of the power, communications and infrastructure systems for reliable emergency operation**

☐ **Power**
- 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
- High amperage/ high voltage systems for such things as x-rays and explosives detection equipment
- Location and capacity of stand-by generators
- Installation of redundant power lines to existing and alternate locations
- Strong consideration to the installation of power lines, or conduit and pull-strings, to known future construction such as expanded terminal concourses

☐ **Cabling Infrastructure Systems & Management**
- Cabling Management
  - Determine standards for type and location of cabling and related infrastructure
  - Determine labeling, color-coding or other identification methods
  - Determine whether to identify security cabling/infrastructure

☐ **Security of Airport Networks**
- Network Availability Considerations
  - Dual (or multi-) network cabling to interconnect mission-critical equipment and platforms
  - The dual network cables may be laid along different paths to minimize the chances of damage
  - Redundant repeaters, switches, routers and power supplies, shall be considered
  - Separate wiring closets may host the redundant equipment
- Network Security
  - Protect networks from unauthorized access by external connections
  - Encryption has important design aspects for securing a general network
  - Shared vs. dedicated fiber is a design/cost issue to be examined with the IT designer
- Network Accessibility
  - WAN connectivity may be a consideration for Internet and/or Virtual Private Network (VPN) access
  - Airport may provide shared networking
- Information Storage Availability
  - Storage systems for mission-critical file server and database should be highly reliable
  - Take into account storage redundancy and back up
  - Pre-allocation of separate facility rooms for redundant storage system equipment
  - Put distance between storage rooms to reduce chances of all rooms being damaged

☐ **Future Rough-Ins/Preparations**
- Comprehensive early planning can significantly reduce future construction costs
- For future terminal expansion, additional concourses and/or gates, new buildings, or expanded or relocated security screening points with known locations, include extra conduit, pull strings, cable or fiber, terminations, shielding and other rough-in elements

☐ **Telecom Rooms**
- Design telecomm rooms, termination closets, wire rooms, in short direct line to each other

- Provide sufficient working space; accommodate known expansion requirements, including 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
- This area will also have additional cooling, fire protection, and dust control requirements

☐ **Radio Frequency (RF)**
- Three broad considerations in using RF-based communications
  - Efficiency and cost
  - Potential interference with other operational elements, including aircraft and air traffic communications, security operations, or general administrative data transfers

☐ **Physical Environment Concerns**
- Weather considerations
- Temperature
- Rain
- Snow
- Dust and dirt

☐ **Regulations - Coordinate with FCC, FAA, and TSA**

☐ **Installation Considerations**
- Antenna location, mounting, and directional/omni-directional considerations
- Other transmitters that have the potential to “interact” with airport systems
- Obstructions
- Coverage areas (and dead spots)
- Robustness of link
- Mobile or Portable
- Shielding
- Effect, if any, on ATC communications

☐ **Communications**
- Access to Main communication bus
- Network Access Security

☐ **Other Considerations**
- Interference is two-way
  - Higher frequency systems have more directional antennas, so emission can be better controlled.
  - “Outside the building” RF environment is unpredictable, requiring internal 'isolation'.
- Choke Effects Integral to Construction
  - At the low frequencies, wavelengths are long and can 'match' terminal openings
  - Subsurface metal rods, I-beams, etc. that ‘surround’ these openings, can create an effective RF choke
  - Adjusting passageway opening size can 'better tune' the choke
- Other Lessons Learned
  - Electrical and electronic environment at commercial airports rarely remains constant
  - There is always more that can be done to improve the EMC status
  - Loading bridge orientation can reduce unwanted radiation

Section I - International Aviation Security and Its Implications for U.S. Airports

1. Impacts on U.S. Airports of Foreign Security Requirements and Initiatives

At its summit meeting in Scotland in July 2005, the Group of Eight (G8) nations agreed to plans and policies for improving travel security and efficiency concerns identified by the Secure and Facilitated International Travel Initiative (SAFTI). The G8 States also agreed to work with the International Civil Aviation Organization (ICAO) to encourage worldwide implementation of these practices.

The extent that ICAO Standards and Recommended Practices (SARPS) will impact U.S. airport design requirements will be determined by the U.S. Department of Homeland Security (DHS) and will be reflected in DHS Technical Requirements transmitted to U.S. airports through existing agency and industry groups.

At the G8 summit, the U.S. has announced an initiative to create the "Smart Border of the Future." According to a White House statement:

> *"The border of the future must integrate actions abroad to screen goods and people prior to their arrival in sovereign US territory, and inspections at the border and measures within the United States to ensure compliance with entry and import permits.… Agreements with our neighbors, major trading partners, and private industry will allow extensive pre-screening of low-risk traffic, thereby allowing limited assets to focus attention on high-risk traffic. The use of advanced technology to track the movement of cargo and the entry and exit of individuals is essential to the task of managing the movement of hundreds of millions of individuals, conveyances, and vehicles."*

2. U.S. FIS and Homeland Security Requirements

If the terminal plan includes a Federal Inspection Service (FIS) area, security design and construction requirements will be determined for the FIS area by U.S. Customs and Border Protection (CBP) and other Federal agencies which will use the FIS to screen arriving international passengers.

FIS facilities are designed according to law enforcement and security situations which are not usually encountered in daily domestic traffic.

The FIS area is defined in terms of passenger and baggage flow and terminal building space utilization. Governmental procedures applicable to the clearance of aircraft, passengers, crew, baggage, and cargo arriving at airports are the outgrowth of United States law, administrative regulations, bilateral treaties and experience.

FIS facilities are required at all U.S. airports which process passengers arriving on international flights who have not been pre-cleared by U.S. agencies at an overseas departure gateway. FIS facilities consist of passenger processing areas for each Federal agency including support spaces for offices, maintenance, telecommunications, and other functions.

FIS areas are also required at pre-clearance and pre-inspection stations located outside of the U.S., where the designated FIS area is the restricted area from the Primary Processing Lane (PPL) to departing aircraft, including all areas in between and support spaces.

Passenger processing facilities are provided by the airport at no cost to the government and inspection services are normally furnished by the government at no cost to the airport. By law, airports are required, at airport expense, to provide adequate passenger and baggage processing space, counters, hold rooms, office space, equipment, utilities, vehicle parking, and other facility-related support required for the FIS agencies to function properly.

FIS space and other requirements will vary according to the CBP Standards for small, medium and large airports. Design of the FIS should reflect the standards and these differences and be coordinated at the beginning of the design process with CBP.

CBP publishes a document, CBP Airport Technical Design Standards, which can be obtained from the local CBP Director of Field Operations. The CBP Airport Technical Design Standards provides facility and security design standards for CBP operational spaces. It is critical to coordinate FIS requirements with CBP in all aspects of design and construction discussions. Where present, written approval should also be obtained from

the Public Health Service Centers for Disease Control and Prevention (U.S. PHS/CDC) and the U.S. Fish and Wildlife Service (FWS) for the space either agency will occupy.

a. CBP's Mission and Requirements

DHS has three core missions:

- To prevent further large-scale terrorist attacks in the United States;
- To better secure critical infrastructure; and, although it assumes failure,
- To prepare for and respond to large-scale terrorist attacks.

CBP's three primary responsibilities at an airport are

- To strictly control the entry of all persons into the United States,
- To assure that individuals, baggage and cargo do not conceal illegal substances or other forms of contraband and,
- At stateside airports, to monitor outbound international traffic assuring that illegal monetary instruments and other controlled articles are not transported across a U.S. border.

Though CBP's priority mission is to prevent terrorists and weapons of terror from entering the United States, the rapid processing of bona fide visitors at U.S. gateways is also a CBP priority.

CBP's responsibilities mandate a thorough screening of each individual, a comprehensive examination of suspect baggage or cargo and an intensified effort to protect American agriculture from the introduction of injurious plant and animal pests and disease.

At selected airports in the United States, the Public Health Service and the Fish and Wildlife Service are also present. The Public Health Service enforces regulations preventing the introduction, transmission and spread of communicable diseases and the Fish and Wildlife Service enforces laws addressing the illegal trafficking of protected fish, wildlife and plants. At larger airports, an investigative bureau of the DHS, Immigration and Customs Enforcement (ICE), may also be present and require office space for agents assigned to the airport.

b. FIS Space Requirements

The size of the CBP passenger processing facility is often determined by the number of passengers processed at the peak hour of operation and by the number of aircraft arriving during a set time period. When these parameters have been established, the airport should contact local CBP officials who will assist in developing specific requirements for each proposed facility.

CBP operational space requirements are set forth in the CBP Airport Technical Design Standards. These technical design standards are minimal criteria deemed practical by existing and projected peak passenger flow in concert with existing or anticipated facility design specifications.

The design and construction of spaces within the secure perimeter of an inspection facility and other related areas controlled by CBP must be approved in writing before inspection services begin. New or renovated passenger processing facilities must comply with all applicable CBP standards in place at the time of construction document approval.

Where present, written approval should also be obtained from the Public Health Service and Fish and Wildlife Service for the space either agency will occupy.

c. CBP FIS Flow Process

The operations and functioning of the FIS are illustrated in *Figure III-I-1* (on page 193) which was developed by CBP. This diagram is a general representation for a majority of airports, however each airport's FIS design will have to reflect the unique requirements and flow process of the respective airport.

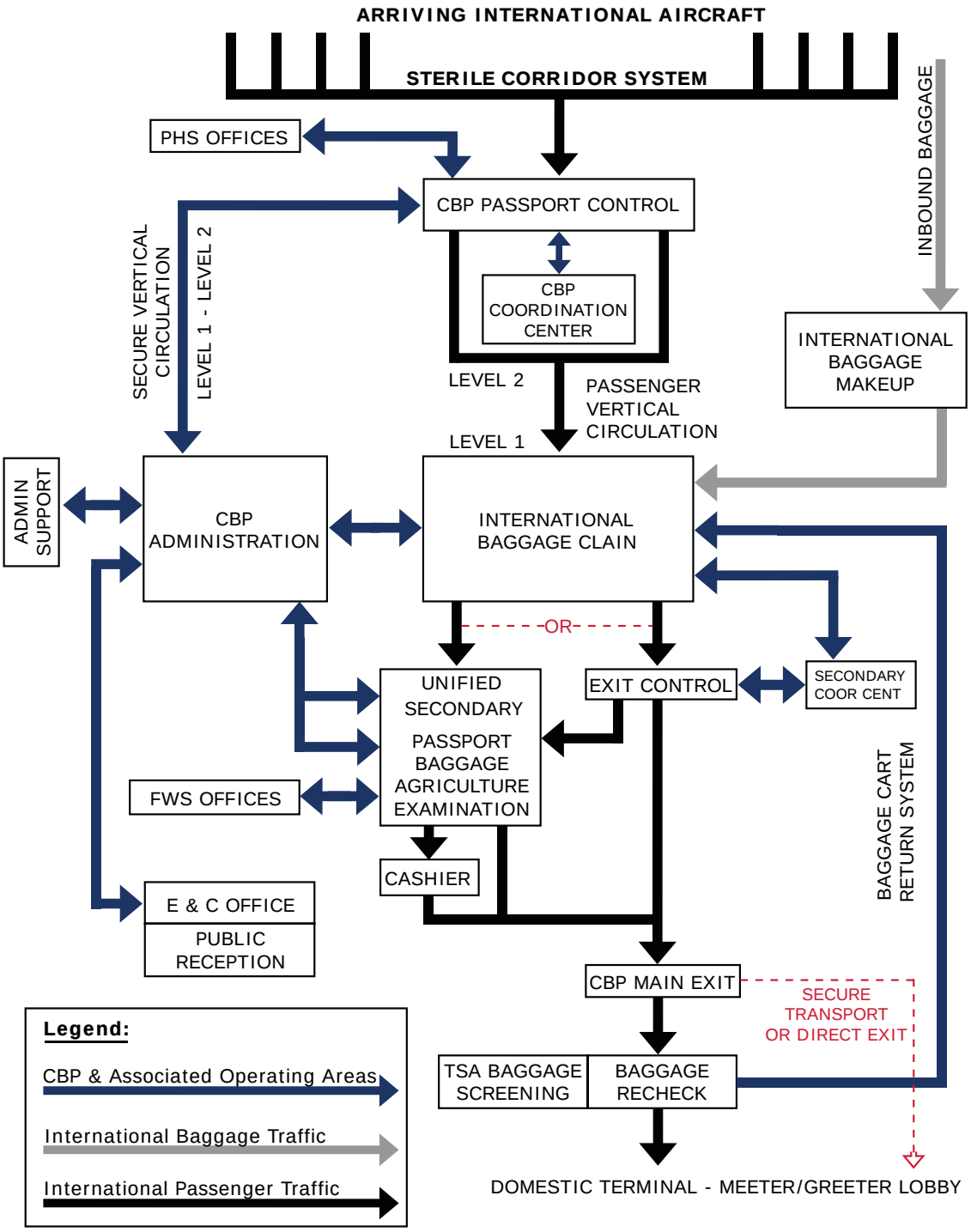


Figure III-I-1 - Flow Process for International Air Passengers Arriving at a U.S. Port of Entry

Once a project has been identified, the CBP Port Director and/or Field Office representative will coordinate with the responsible CBP Headquarters personnel and provide all pertinent project information, including timelines and points of contact.

Facility planning and design review is a joint responsibility of the CBP Field Office, Headquarters Office of Field Operations, Headquarters Office of Finance Portfolio Management Division, and the Office of

Finance National Logistics Center. However, the CBP Office of Field Operations is the final authority for approving all construction projects.

Other FIS agencies including the Fish and Wildlife Service and the Center for Disease Control Public Health Service need to be contacted and consulted for additional requirements and processes.

At a stateside airport the secure perimeter is comprised of international gates, the sterile corridor system, processing areas, in-transit and VIP lounges, administrative offices and admin support spaces. Related areas include aircraft parking ramps, hardstands, baggage handling areas and international outbound interview rooms.

At a U.S. pre-clearance site the secure perimeter encompasses processing areas, baggage drop conveyors, outbound passenger holdrooms, administrative offices and admin support spaces. Related areas include aircraft parking ramps and the inspected baggage hold room. Refer to the CBP Airport Technical Design Standards for specific information regarding pre-clearance facility requirements.

In the initial stages of planning, an airport should allow at least 80 square feet per peak hour international deplaning passenger, assuming an aircraft load factor of 90 percent. A 215-seat aircraft, for example, will require space to service 194 peak-hour international passengers, or 15,500 square feet of FIS space. CBP must be consulted early in the planning stages of a project to determine specific space and operational requirements.

Depending on how an airport terminal is configured and how gates are assigned to arriving international flights, secure passageways may also be required to route deplaning passengers to the FIS area from the gates. These passageways, also known as sterile corridors, will need to be secured as part of the FIS with CCTV cameras, access control readers, and such other security devices as required by the FIS security design requirements.

When an inspection facility has been completed and accepted for occupancy, all areas within the secure perimeter fall under the sole control of CBP. CBP officials must authorize all physical access by airline or airport employees and any future alteration or addition to the facility.

All of these requirements should be reviewed in meetings with CBP representatives early in the facility planning process.

d. CBP Airport Design Review and Construction Management Process

The steps involved in establishing FIS design requirements begin when CBP receives an airport's request for an FIS facility construction project. CBP will review the airport's request to determine FIS operational and technical requirements, and will provide approval(s) as required. Once CBP's requirements are provided to the airport, the design process begins and progresses through design development until a set of construction documents is ready for bid. CBP must be closely coordinated with throughout the design process for the FIS spaces, and this coordination must continue through construction, acceptance, occupancy, and commissioning.

CBP expects this process, which CBP calls the Airport Design Review and Construction Management Process, to proceed in the following manner:

1) CBP receives notification and request for an FIS facility construction project from the airport operator and in some cases a carrier.
   - Minimum CBP, Airport Operator/Carrier Responsibilities: Airport Operator/Carrier submits request to build an FIS facility to CBP including the following information: Number of/frequency of flights, Number of gates, originating countries, passenger load including passengers per hour on opening day and projected passenger traffic for 5 and 10 years after opening, and a feasibility study (if completed).

   CBP reviews and coordinates the airport request within CBP to determine feasibility and provides approval(s) to airport operator/carrier as required. CBP provides requirements to the airport operator/carrier.

2) Pre-Design and Programming
   - Minimum CBP, Airport Operator/Carrier Responsibilities: Airport Operator/Carrier A/E begins pre-design and programming and coordinates with CBP for required CBP reviews and approvals regarding space programming, site selection, concept development, functional adjacency, blocking/stacking diagrams, and facility long-term master plan.

3) Schematic Design
   - Minimum CBP, Airport Operator/Carrier Responsibilities: Airport Operator/Carrier/A&E begins schematic phase and coordinates with CBP for required CBP reviews and approvals regarding room layout, specifications, technical narratives (engineering systems), floor plans/sections, and elevations.

4) Design Development.
   - Minimum CBP, Airport Operator/Carrier Responsibilities: Airport Operator/Carrier/A&E begins design development phase and coordinates with CBP for required CBP reviews and approvals regarding floor plans/sections, elevations, finish schedules, engineering system single line diagrams (all building systems), security systems layout, special construction requirements (detention rooms, search rooms, storage rooms, etc.), reflected ceiling plan, booth and counter drawings.

5) Construction Documents
   - Minimum CBP, Airport Operator/Carrier Responsibilities: Airport Operator/Carrier/A&E begins construction documents phase and coordinates with CBP for required CBP reviews and approvals regarding floor plans/sections, elevations, finish schedules, door schedules and door access control points, door hardware sets and specifications, engineering system single line diagrams (all building systems), security systems layout, special construction requirements (detention rooms, search rooms, storage rooms, etc.), computer room rack layouts, and booth and counter drawings.

6) Construction Phase
   - Minimum CBP, Airport Operator/Carrier Responsibilities: Airport Operator/Carrier/A&E begins construction phase and coordinates with CBP for required CBP reviews, establishment of punch-list, and approvals regarding bid/award update, construction phase kick-off, construction schedule and milestones. Any deviation from CBP approved construction documents must be reported to CBP.

7) CBP Acceptance, Occupancy, and Commissioning
   - Minimum CBP, Airport Operator/Carrier Responsibilities: Airport Operator/Carrier/A&E proceeds to move-in/occupancy phase and coordinates with CBP for required CBP reviews and approvals regarding furniture, computer, and equipment install, resolution of punch-list, staff move-in and commissioning for first flight arrivals.

Processes may vary depending on the FIS project scope and requirements at each airport. CBP strongly recommends that airports consult with CBP early in the planning stages of any FIS project.

e. Airport & A&E Responsibilities for the Design and Provisioning of FIS Facilities

Airports and their architects-engineers (A&Es) are responsible for the design, construction, outfitting, and support of space layouts, physical security, communications, cable plants, and other support functions for the FIS.

The airport and its A&Es are also responsible for coordinating FIS space and facility requirements with local and national building/engineering codes, with requirements as the Americans with Disabilities Act (ADA), and with other Federal, State, and local statutory requirements.

It is critical to coordinate FIS requirements with CBP in all aspects of design and construction discussions. It is critical for airport authorities considering the construction of a new or the renovation of an existing passenger processing facility will involve CBP and other FIS agencies during all stages of project planning, design, construction and occupancy. Failure to do so often results in improper compliance with mandatory application procedures and unacceptable design assumptions that can cause significant time delays and increase construction cost.

f. Airport FIS Planning and Design Issues

Some of the FIS design issues which an airport and its A&E need to resolve early in the planning process for the FIS are:

- FIS Security Plan: The airport will need a security plan for the FIS from which to develop construction specifications and drawings. CBP encourages airports to engage with CBP experts as early in the planning process as possible, and to draft a security plan which addresses:
  - Protection strategies;
  - Planned safeguards, such as partitions, locks, cameras, et al to ensure the sterility of the FIS area including any required pathways;
  - Plans and procedures for implementing, managing, and maintaining the planned security safeguards;
  - Resources needed to sustain the FIS protection program;
  - Security personnel qualifications, locations, hours of operation and specific duties; and
  - Designated evacuation routes, assembly areas and associated planning, procedures, and staffing.

- Detailed Drawings: FIS agencies may provide typical drawings and written specifications, but the A&E must adapt these and integrate them into the actual facility design. That requires CBP and other FIS agency component involvement through initiation by the airport.

- Design and Equipment Standards, Specifications, and Equipment Requirements: All parties must agree on which standards and specifications are binding, which can be implemented with a "best practices" approach, and how best to select and outfit equipment for the FIS.

- System Integration and Networking: In the past, FIS facilities were designed to be stand-alone operations, using dedicated cable plants and equipment and with minimal support from airport systems and airport data networks. This model is likely to continue, however, the advent of new technologies, including wideband data networks capable of transmitting live video images and packet-based voice telephony (also known as VoIP, or Voice over Internet Protocol), integration with airport systems may result in a more cost-effective design at some airports. It is now common practice for an airport's card access control system to also be used for FIS access control, with permissions controlled in software according to the role and responsibility of the cardholder. It is also common practice for imagery from airport surveillance cameras to be shared with CBP.

  The expanding use of biometrics for traveler authentication and increased use of video surveillance systems will encourage even greater integration in the future. Data networking may also provide the opportunity for improving security now that means have been developed to isolate the data traffic of

multiple stakeholders riding on a common network. These means include virtual local area networks (VLANs), intrusion detection appliances, and data encryption. The government's new Advanced Encryption Standard (AES) secures data in all transmission modes and is to be used by all Federal agencies for classified material. Airports and the FIS agencies need to explore how such advances can be leveraged to improve FIS operations while reducing the airport's construction costs.

- CCTV and the Physical Security System: An airport CCTV system is designed to perform two functions, assessment and surveillance. Assessment cameras are used by both CBP coordination center operators and airport security to assess threats posed by alarm events. Surveillance cameras are used by airport security to monitor activity both inside and outside the terminal. CBP employs agency dedicated surveillance cameras at stateside airports to monitor arriving international passengers, air crew members and baggage and cargo carried aboard from deplaning to and through processing. At pre-clearance sites these cameras are used by CBP to monitor activity in the processing area, in the inspected passenger and baggage holdrooms and on the U.S. bound aircraft parking ramps.

  At certain airports, CBP officials may require unique CCTV design considerations and should be consulted during all FIS Physical Security System (PSS) planning. Major components of the CCTV system must be capable of full color transmission although black and white cameras are commonly employed where additional light sensitivity is required. Pan/tilt/zoom (PTZ) cameras are used to supplement fixed cameras permitting more accurate coverage in critical areas.

  The CBP coordination center must also have a minimum of one high definition digital video recorder capable of recording or playing back any camera view. All camera views associated with an alarm must be automatically recorded.

  In a number of cases CBP, airport security and the airlines can share camera views with two notable exceptions. Only CBP personnel are permitted to view cameras observing the inspection process. This precludes anyone viewing the output of a stateside facility camera located between primary queuing and the main exit or between baggage claim and baggage drop at a pre-clearance site. In addition, CBP must have exclusive monitoring access to the stand alone secondary CCTV system that allows CBP officers to monitor detainees in interview rooms, holdrooms and expedited voluntary removal rooms. Coordination center operators must also be able to take sole control of all shared PTZ cameras associated with an international deplaning. All CBP non-sensitive camera views should be transferable to airport security when the facility is closed and retrievable when it reopens.

- Access to FIS Areas: Policies and procedures for allowing airport Operations and other airport personnel to restricted FIS spaces needs to be programmed into the access control system prior to the facility opening. FIS agencies must notify airport Operations as to which cardholders will be granted access, and the Airport Security Plan (ASP) will have to reflect this procedure.

  CBP must have complete control of access to CBP sterile areas typically by providing an authorization code defining multiple sterile area access levels which are inserted into a database of authorized persons. The capability of providing this code is restricted to selected CBP personnel. No modifications can be made by others in subsequent ID media procedures. The ID media includes the appropriate Department of Homeland Security (DHS) seal on a contrasting background permitting prompt recognition of unauthorized persons entering or transiting the CBP sterile area.

  The access control system must provide Customs and Border Protection with the ability to immediately invalidate an individual's access code when access to the sterile area has been revoked and trigger the issuance of a new media without the DHS seal if the individual is still authorized access to other restricted areas of the airport. Larger airports may be required to provide the CBP coordination center with an ID media system computer capable of transmitting information to and receiving information from the Airport Security Command Center. All ID media are issued and database changes made by the airport security staff.

- Expanding Footprint: CBP is increasingly concerned about activities exterior to the FIS at ramps, other areas in the vicinity of the FIS, the movement of baggage carts and the unloading of baggage onto carousels. This expanded footprint will require additional video surveillance and

communications capabilities. CBP will want to monitor and control such activities from a central point within the FIS, the CBP Coordination Center. The FIS footprint will also be expanded to address FIS activities during emergencies, such as having to evacuate the FIS when an aircraft is still unloading and some passengers are being processed in the FIS areas while other passengers are waiting to deplane.

- Traveler Authentication: The DHS US-VISIT program, begun in 2004, employs biometric techniques to verify an individual's identity, and to confirm that he or she is who they profess to be. This measure adds approximately 15 seconds to the inspection process. The objective of the program is to check the status of foreign nationals entering the country and assure that no one overstays his or her admission period. Airport security access control planning should be compatible with biometric techniques used in the FIS.

g. Lessons Learned from U.S. Airports

CBP has developed technology to model passenger flow in an FIS area. This information can be used to optimize the space layout and thereby result in an optimum construction plan.

The CBP inspection flow program is known as the Workforce Analysis Model (WAM). The WAM uses data unique to the airports to derive the projected maximum peak volume (MPV) of arriving international passengers in one hour. Four design/installation rope options considered include:

- Non-symmetrical design
- Nonsymmetrical with buffers
- Symmetrical design
- Symmetrical design with buffers

After reviewing the results of prior simulations, the following observations were made:

- None of the designs can be ranked best under all conditions.
- Queue designs with buffers always performed better than those without.
- Non-symmetrical queue designs provide maximum room for non-citizen queuing.
- Symmetrical designs provide increased queue space for citizens but reduced non-citizen queue space.
- Queue rope use provides a more uniform waiting environment with improved processing times.
- A symmetrical queue design with buffers provides the best overall passenger flow with less congestion.
  - Organized queues provide a better perception that progress is being made.
  - A similar simulation of the FIS processes was done for the Houston Intercontinental Airport. This second analysis supported the key observations listed below:
    - Average aircraft processing time through Primary was 16.7 minutes.
    - Only two of 356 flights processed exceeded 45-minutes.
    - The average passenger delay through Primary was 5.8 minutes.
    - Staffing simulated was adequate for processing the demand.
    - When Primary processing time was decreased, a corresponding increase in bag claim time was recorded. No net reduction in passenger transit time was observed.
    - A modified WAM model detailing the total FIS process was provided for analysis.

The following "lessons learned" are provided courtesy of the Houston Airport System, based on FIS experiences at the Bush International Terminal in Houston.

#1: Thoroughly Model the Proposed Design
- Don't underestimate the need for clear and unambiguous passenger flow.
- Model various CBP staffing possibilities and variability of available personnel.
- Model variability in processing times and passenger flow through exit control.

#2: Life Safety Issues vs. Security Requirements
- Prior to 9/11 life safety had precedence over security.
- Post 9/11 life safety and security have equal footing.
- Compromises can be time consuming and costly.
- Establish a task force to review the project, establish design review, set design parameters, and define dispute resolution protocol

#3: Establish Agency Facility Requirements.
- Take time in the programming step to meet with each agency.
- Obtain documented agreement on facility requirements.
- Establish single decision authority from each agency for standards.
- Address in detail requirements related to architecture/MEP, security, and IT.

#4: Changes Will Occur / Establish Protocols
- Have mechanism available for procuring additional funding.
- Establish a process for reviewing and accepting/rejecting changes.
- Document each change and specify the reason for the change for project evaluation.

Section III-I - International Aviation Security Checklist:

☐ **Establish Security Plan for FIS**
- Contact CBP and other Federal Agencies
  - Obtain CBP Airport Technical Design Standards
  - Obtain Workforce Analysis Model (WAM).
- Address CBP Issues in FIS Security Plan
  - Protection Strategy
  - Physical Safeguards
  - Plans and Procedures for Implementation/Management
  - Resources Required to Sustain FIS Protection Program
  - Evacuation Routes, Assembly Areas, Staffing
- Coordinate FIS Security Plans and Requirements with Airport Security Plan (ASP)
  - Access Control
  - CCTV
  - Baggage Screening and Explosives Detection
  - Perimeter Protection, including blast protection
  - Video, Voice, and Data Networking

☐ **FIS Design, Construction, Acceptance and Occupancy**
- Provide for CBP/Agency Involvement in Design and Construction Process
- Design Specifications, Drawings, and Construction Documents
  - Schematic Design
    - Model variability in processing times and passenger flow through exit control using the CBP Workforce Analysis Model (WAM) to size FIS
    - Architectural Integration
    - Security Integration
    - IT Integration
  - Design Development
  - Construction Bid Package
  - Obtain written approval(s) from CBP/Agencies at each step in this process
- Establish Change Review/Approval Process with CBP
- FIS Inspection and Acceptance
- FIS Occupancy

PART IV

APPENDICES

DISCLAIMER

The following appendices and supplementary materials provide additional information in support of the guidelines and recommendations contained throughout this document. Like the underlying document, these appendices are not intended to contain regulatory or mandatory language, except as they might make occasional informational reference to external documentary resources. These appendices do not supplant or modify any statutory or regulatory requirements applicable to airport operators. This document is expected to have a multi-year useful life, and therefore might occasionally refer to information that has since been superseded, amended or modified. In such cases, the reader is referred to the most recent version of those resources for further guidance. The various analytical models are presented in summary form, and are intended only as an introduction to the actual models that are available both from government and private industry sources, each of which might approach the analytical process from somewhat different perspectives. The object of this document is not to provide the designer or architect with a definitive solution to each site-specific problem; nor to specifically endorse any product or approach. Rather, it is to make the reader aware of the existence of various opportunities available for gathering additional information, and to provide the reader with a broader frame of reference for a better-informed and balanced decision–making process.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

AIRPORT VULNERABILITY ASSESSMENT PROCESS

Section A - The Vulnerability Assessment

An airport vulnerability assessment is the key tool in 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 that as a more expensive retrofit.

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.

Thus, security is a process of risk management, identifying major threats and considering how vulnerable the system might be to the actions they threaten.

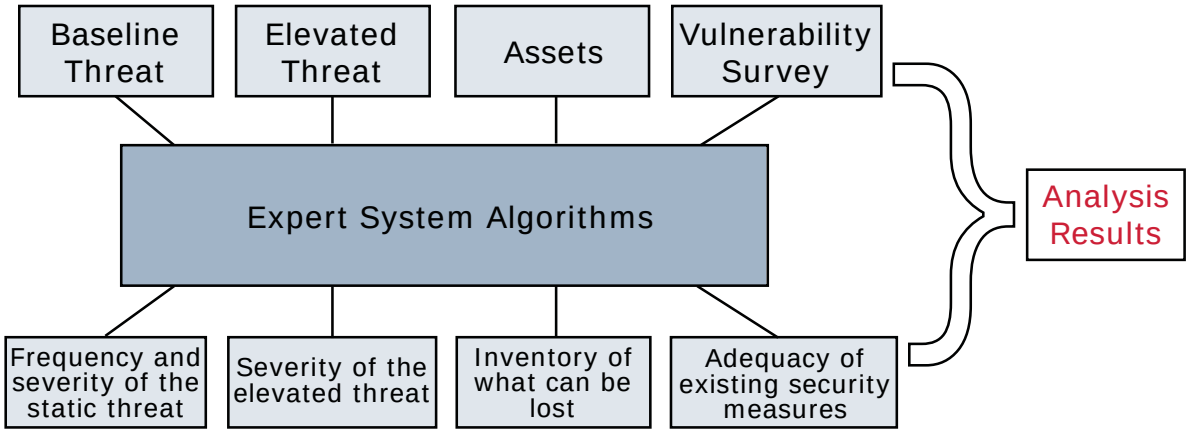
Threats are defined as specific activities that will damage the airport, its facilities, or it patrons. Threats include any actions which detract from overall security, and range from the extreme of terrorist-initiated bombs or hostage-taking to more common events such as theft of services, pick-pocketing, 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.

Vulnerability is defined as the susceptibility of the airport and its systems to a particular type of security hazard. Vulnerabilities can be corrected, but risk analysis must be undertaken to determine which vulnerabilities take the highest priority.

Presently there are a number of vulnerability assessment tools and methodologies available from government and private organizations. All of these tools are subjective to varying degrees.

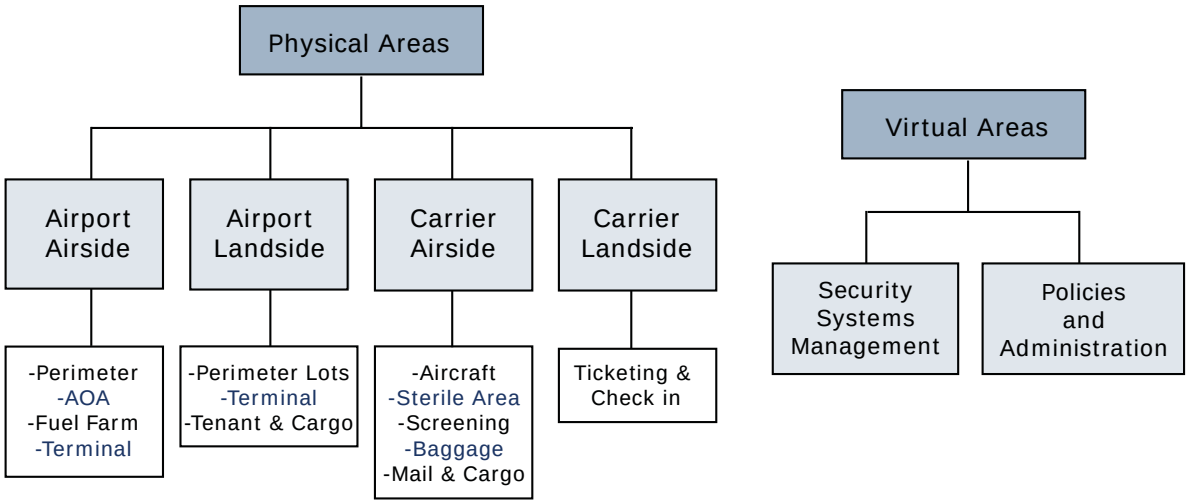
Following the Pan Am103 and TWA 800 incidents, the FAA embarked on the development of a Civil Aviation Security Risk Assessment Program (CASRP). The objective of this program was to provide a tool to quantify security risk, to provide consistent assessments, and to support recommendations for specific improvements to the security of individual airports and airlines.

Appendix A Figure A-1 below is a top-level diagram of the architecture of CASRAP. As shown in the figure each of the elements of a CASRAP risk assessment interacted with an expert system which included analysis algorithms. These algorithms made judgments about the frequency and severity of threats, attractiveness and value of assets, and adequacy of existing security measures and displayed this information to users in easy to read charts.



Appendix A Figure A-1 - CASRAP Assessment Model

CASRAP also provided a schematic for assessing vulnerabilities, which is shown in *Appendix A Figure A-2* below.



Appendix A Figure A-2 - Model for Assessing Vulnerabilities

Following 9/11, the Transportation Security Administration (TSA) developed a self-assessment application, known as the Vulnerability Identification Self Assessment Tool (VISAT), a voluntary web-based toll which enabled owners and operators to rate their security systems. The tool was developed by TSA's office of threat assessment and risk management to get a handle on the enormous challenge of securing the transportation sector by soliciting data from the owners and operators of transportation-related assets. TSA planned to use the information to prioritize their resources, but stressed that VISAT was only one part of an overall risk management strategy.

The tool consisted of two parts. In the first part, users answer a series of questions related to their security posture, including queries about their security training, access control, physical security assets, security technologies and

equipment, communication security and information security. The second part of the VISAT module focused on the prevention of terrorist attacks under various scenarios. "Users rate their asset in terms of target attractiveness (from a terrorist's perspective)," stated the Federal Register notice. "Users first list the assets baseline security countermeasures that apply for each of the threat scenarios, and then rate the effectiveness of the countermeasures in detecting and/or preventing the terrorist's actions against each threat scenario." Once the assessment is completed the user receives a report highlighting vulnerabilities and develops a security plan. This assessment can be submitted to DHS for additional feedback.

TSA is in the process of determining the most effective way to evaluate airport vulnerabilities based on threat assessments. Until this process of review is completed, it is suggested that airport vulnerability assessments continue to be conducted, as they have been, through a structured self-assessment process and in the context of vulnerability guidance issued by other government agencies. This includes analyses conducted by appropriate law enforcement agencies (federal, state and local) in conjunction with the local airport authority, local airport law enforcement department, local FSD, and all other appropriate stakeholders.

The performance of a vulnerability assessment should be a coordinated effort of the airport authority, the airport security coordinator, and local FSD to assure that the recommended actions are considered and factored into airport design efforts.

Airport planners and designers should be aware of and take advantage of threat and vulnerability assessment methodologies, guidelines, and standards developed by U.S. government agencies, several examples of which are cited in the *Bibliography* Appendix. These sources include the DHS FEMA preparedness, facility protection, and post-attack primers; Department of Transportation (DOT) guidelines for transit system security; General Services Administration (GSA) guidelines for government building structures; Department of State (DoS) standards for international facilities; Department of Defense (DoD and U.S. Army Corps of Engineers standards and specifications for military facilities; and federal, state, and local law enforcement agencies with the FBI having a special role for threat-related data.

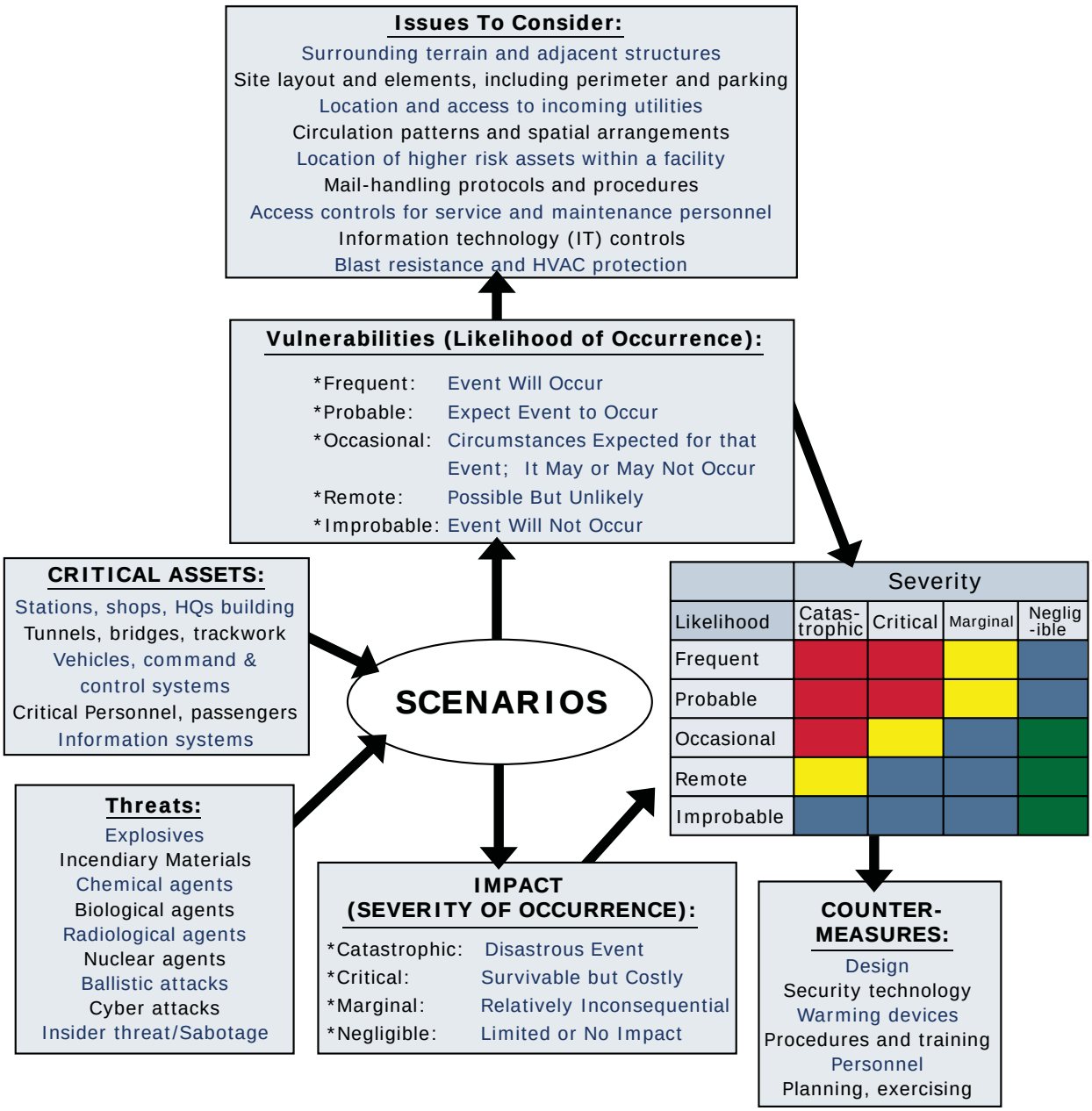
The discussion that follows has been synthesized from many of these sources.

Section B - The Assessment Process

Threat and vulnerability assessment provides 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.

The threat and vulnerability assessment process is conceptually diagrammed in *Appendix A Figure B-1* for a transportation system. These assessments typically use a combination of quantitative and qualitative techniques to identify security requirements, including historical analysis of past events, intelligence assessments, physical surveys, and expert evaluation. When the risk of hostile acts is greater, these analysis methods may draw more heavily upon information from intelligence and law enforcement agencies regarding the capabilities and intentions of the aggressors.

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 49 CFRs and industry-recommended best practices.



Appendix A Figure B-1 - Model for Assessing Vulnerabilities

Effective assessments typically include five elements:

1. **asset analysis;**
2. **target or threat identification;**
3. **vulnerability assessment;**
4. **consequence analysis (scenarios); and**
5. **countermeasure recommendation.**

1. 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 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?

2. 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.

Threat analysis defines the level or degree of the threats against a facility by evaluating the 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 are displayed below.

- 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 *Appendix A Table B-1* below. Historical examples are provided for reference and consideration, as well as to illustrate the types of weapons typically used in these attacks.

Appendix A Table B-1 - Examples of Terrorist Attacks and Weapons

Type of Attack	Historical Example	Types of Weapons
Explosive and Incendiary Devices	1995 - GIA bombing of Paris Metro	Planted Devices
	HAMAS suicide bombs on Israeli buses	Suicide Bombs
	1998 - bombings of U.S. embassies in Tanzania and Kenya	Vehicle Bomb
	2001 - World Trade Center; 1990s - abortion clinic bombings in GA; 1995 - Oklahoma City Bombing	Proximity Bombs; Incendiary Devices; Secondary Devices
	2002 and continuing - suicide bombings in Iraq 2005 - suicide bombing of Jordanian hotel	Vehicle Bomb; Concealed Body-worn Plastic Explosives
Exterior Attacks	2001 - militant assaults on Indian-held mosques in Kashmir	Rocks and Clubs; Improvised Devices; Molotov cocktails
Stand-off Attacks	Tamil Tiger's July 2001 mortar attack & bombing of Sri Lanka's National Airport	Anti-tank rockets; Mortars
Ballistics Attacks	Long Island Railroad Shootings; Columbine High School	Pistols; Handguns; Submachine guns; Shotguns
Networked/Inside Access: Forced Entry Covert Entry Insider Compromise Visual Surveillance Acoustic/Electronic Surveillance	Amtrak Sunset Limited derailment 1996 Tupac Amaru Revolutionary Movement taking of Japanese Ambassador's resident and 500 guests in Peru (access through disguised as waiters at the party)	Hand, power and thermal tools; Explosives
		False credentials; Stolen uniforms and identification badges
		False pretenses, cell operations
		Binoculars; Photographic Devices
		Listening Devices; Electronic-emanation surveillance equip.
Cyber Attack	Code Red Worm (2002)	Worms, Viruses, Denial of Service Programs
Chemical, Biological, Radiological, & Nuclear (CBRN) Agent Release	1995 - Aum Shinrikyo Sarin Gas Release in Tokyo Subway	Chemical, biological, or radiological or nuclear aerosolized

3. Vulnerabilities

Vulnerability is anything that can be taken advantage of to carry out a threat. This includes vulnerabilities in the design and construction of a facility, in its technological systems, and in the way a facility is operated (e.g., security procedures and practices or administrative and management controls).

Vulnerability analysis identifies specific weaknesses with respect to how they may invite and permit a threat to be accomplished.

Vulnerabilities are commonly prioritized through the creation of scenarios that pair identified assets and threats. Using these scenarios, transportation agencies can evaluate the effectiveness of their current policies, procedures, and physical protection capabilities to address consequences.

4. Scenario Analysis

Scenario analysis requires an interpretive methodology that encourages role-playing by transportation personnel, emergency responders, and contractors to brainstorm ways to attack the system. 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 preformed to recognize, prevent, and mitigate the consequences of attacks. *Appendix A Table B-2* below lists examples of likely threats to airports.

Appendix A Table B-2 - Examples of Likely Threat Scenarios

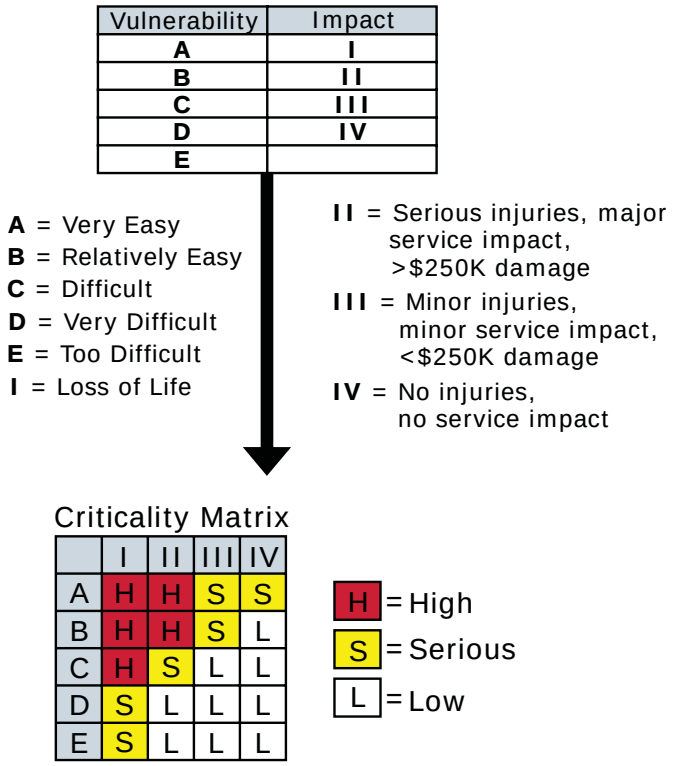
Assets	Most Probable Threats
Terminals	- High-yield vehicle bomb near terminal - Lower-yield explosive device in terminal - Armed hijacking, hostage, or barricade situation in terminal - Chemical, biological, and nuclear release in terminal - Secondary explosive device directed at emergency responders
Fuel Storage Facilities	- Explosives detonated in or near fuel facilities
Security Operations Centers	- Physical or information attack dispatch system - Armed assault, hostage, or barricade situation - Explosive device near or in Operations Control Center - Sabotage of vehicles or maintenance facility

The FBI recommends that transportation systems focus on the top 10% of identified critical assets (at a minimum). Using these assets, transportation personnel should investigate the most likely threats, considering the range of attack objectives and methods that may be used (such as disruption of traffic, destruction of bridge or roadway, airborne contamination, hazardous materials accident, and threat or attack with explosives intended to disrupt or destroy). The airport 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 worse case scenario.

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, serious, and low.

Consequences are assessed both in terms of severity of impact and probability of loss for a given threat scenario. *Appendix A Figure B-1* below shows one process for accomplishing this.



Appendix A Figure B-1 - Scenario Evaluation Criteria

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, use the scenarios 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);
- 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
- Information technology (IT) and computer network ease-of-penetration

At the conclusion of the scenario-based analysis, the airport should have assembled a list of prioritized vulnerabilities for its top 10% critical assets. Typically, 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).

5. Developing Countermeasures

Based on the results of the scenario analysis, the airport 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 different countermeasures are available to protect an asset?
- What is the varying cost or 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 should not be placed right next to the building's reception area, rather 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 electronic access control, intrusion detection, closed circuit TV, 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.

a. *Appendix A Table B-3* below lists countermeasures that should be considered to reduce and mitigate airport security vulnerabilities.

Appendix A Table B-3 - Vulnerability Countermeasures

COUNTERMEASURES	Planning	Coordination with Local Responders	Training and Exercising	Physical Security: Access Control	Physical Security: Surveillance	Physical Security: Blast Mitigation	Physical Security: WMD Agent Protection
Identifying Unusual or Out-of-Place Activity	X		X	X	X		X
Security Screening and Inspection Procedures	X	X	X		X	X	X
Enhancing Access Control for Vehicles	X	X	X	X	X	X	
Securing Perimeters for Non-Revenue Areas	X			X	X		
Denying Access to Authorized-Only Areas	X		X	X	X		
Securing Vulnerable Areas (target hardening)	X			X	X	X	
Removing Obstacles to Clear Line-of-Sight	X			X	X		
Protecting Parking Lots	X			X	X		
Enhanced Access Control for SOC & Telecom Rooms	X			X	X		
Securing Critical Functions and Back-ups	X			X	X		
Promoting Visibility of Uniformed Staff	X			X	X		
Removing Spaces that Permit Concealment	X			X	X		X
Reinforcing Natural Surveillance	X			X	X		
Procedures for Vehicle and Terminal Evacuations	X	X	X			X	X
Coordination with Community Planning Efforts	X	X	X				X
Backing up Critical Computer Systems	X		X				
Revising Lost-and-Found Policies	X		X				X
Securing Tunnels and Elevated Structures	X		X	X	X	X	X
Elevating/Securing Fresh Air Intakes	X			X			X
Protecting/Backing Up Incoming Utilities	X			X	X	X	X

Section C - Reducing the Vulnerability of Structures

The U.S, General Services Administration (GSA) has developed its "Progressive Collapse Analysis and Design Guidelines for New Federal Office Buildings and Major Modernization Projects" to ensure that the potential for progressive collapse is addressed in the design, planning and construction of new buildings and major renovation projects. The Guidelines, initially released in November 2000, focused primarily on reinforced concrete structures and was subsequently upgraded to address the progressive collapse potential of steel frame structures.

The GSA Guidelines provide a *threat independent* methodology for minimizing the potential for progressive collapse in the design of new and upgraded buildings, and for assessing the potential for progressive collapse in existing buildings. It should be noted that these Guidelines are not an explicit part of a blast design or blast analysis, and the resulting design or analysis findings cannot be substituted for addressing blast design or blast analysis requirements during threat and vulnerability assessments.

The GSA Guidelines should be used by all professional architects and structural engineers engaged in the planning and design of new airport facilities or building modernization projects.

Section D - Example of a Terrorism Vulnerability Self-Assessment - the FBI Model

The FBI has established the following criteria for targeted facilities which should consider themselves at a high level of risk:

- Facilities having a symbolic meaning for the U.S. government or the national culture and way of life;
- Facilities with precursor elements for major destruction (chemical, nuclear, or radiological material);
- Facilities whose destruction would provide the potential terrorist element (PTE) with visibility and prestige;
- Facilities with the potential to significantly impact not only a single community, but also a state and the nation;
- High-value facilities, e.g., high replacement costs, high commercial impacts of delay and destruction, high loss on U.S. economy;
- Major facilities that provide relative ease of access (for ingress and egress with equipment and personnel required for attack); and
- Facilities that would produce mass casualties (in excess of 500 persons).

In a cooperative partnership with state and local law enforcement, the FBI has requested that such facilities complete a vulnerability self-assessment, emphasizing the above characteristics for each community, using the format described below.

This FBI vulnerability self-assessment model is intended to help a transportation organization determine its vulnerability to terrorism, and to assist local law enforcement in assessing the overall vulnerability of the community. It provides a worksheet that can be customized to the transportation specific organization and is intended to be a general guide. It may not include all issues that would be considered in every specific operation. Therefore, it is imperative that an airport consider the unique character of its functions, its inter-relations with other community organizations, its general public image and its overall public visibility. Consider both who may work in the organization and what the organization does. Assess the symbolic value of the organization to the public.

Each worksheet section is ranked on a 20-point scale. Answering this self-assessment is a subjective process. It should be completed by the person(s) that best knows the physical security and community value of the transportation organization.

There are no firm guidelines on how to score a category. The score can best be determined by the person selected to complete the self-assessment, based on the uniqueness of the transportation organization. Since the questions are subjective, give your "best estimate" when scoring each question.

It is important to remember that the most important threat reduction measure is vigilance on the part of the transportation organization's staff, their awareness of anything out of the ordinary and their prompt communication of that information to the organization's security team or management.

This assessment follows the exact same format of the community assessment performed by local law enforcement to assist in preventing criminal acts committed by terrorists. Based on the results of this assessment, the transportation organization may wish to share a copy with law enforcement, or to include their representative in the assessment process, to support their understanding of the transportation function and role in the community.

This assessment should be conducted at least annually, and again, if there is an increased threat of a terrorist event or whenever there is a significant change to the organization's facilities or activities.

Upon receipt of a "high risk" assessment, each law enforcement agency Sheriff, Chief, or head, or his designated representative may forward that assessment, or other threat report, to the State Emergency Management Agency (or equivalent), to State law enforcement, or to the local Federal Bureau of Investigation office.

TO COMPLETE THE ASSESSMENT:

Circle your evaluated score on each scale for each question. Then total the scores and enter the total on the last page. Based on the total, use the score guide to assign an overall ranking to the transportation organization.

Section A - Potential Terrorist Intentions

⇐ ***Low*** *Vulnerability*																			***High*** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Are you aware of any terrorist threat to your organization?
- ❒ Are you aware of a history of terrorist activity in your area or your specialty?
- ❒ Are you aware of the level of capability of any suspected terrorist which you believe poses a threat to your organization?

Section B - Specific Targeting

⇐ ***Low*** *Vulnerability*																			***High*** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Have you obtained current information from law enforcement or other sources that your organization has been targeted by terrorists?
- ❒ What is the reliability of these information sources?
- ❒ What is your organization's public visibility?
- ❒ Does the nature of your organization's activity lead you to think it may be targeted?
- ❒ Are there activities that indicate possible terrorist preparations in your area or specialty?

Section C - Visibility of your Facility/Activity within the Community

⇦ **Low** *Vulnerability*																		**High** *Vulnerability* ⇨	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Is your organization well known in the community?
- ❒ Do you regularly receive media attention?
- ❒ Is your organization nationally prominent in your field or industry?
- ❒ Is your location and is the nature of your activity known generally to the public?
- ❒ Have you ever had an event or accident with potential health risks that attracted public attention to your facility?

Section D - On-Site Hazards

⇦ **Low** *Vulnerability*																		**High** *Vulnerability* ⇨	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Are hazardous materials, explosives or other dangerous items on your site?
- ❒ Do you store or use biologic or chemical materials that have the potential to be used as a threat or weapon?
- ❒ Do you store or use radioactive material at your site?
- ❒ Do you have a system to control access to hazardous materials, explosives or any other dangerous materials at your site?
- ❒ Can any products stored or used on your site be used as, or in the manufacture of a mass casualty weapon?
- ❒ Can any products stored or used on your site cause extensive environmental damage?

Section E - Population of Site/Facility/Activity

⇦ **Low** *Vulnerability*																		**High** *Vulnerability* ⇨	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Do you have more than 250 people normally present at your site?
- ❒ Do you have more than 1,000 people normally present at your site?
- ❒ Do you have more than 5,000 people normally present at your site?
- ❒ Do you hold events at your site that attracts large crowds?

Section F - Potential for Mass Casualties

⇐ **Low** *Vulnerability*																			**High** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Do materials stored or used at your site have the potential to create mass casualties on-site?
- ❒ Do materials stored or used at your site have the potential to create mass casualties within 1 mile of your site?
- ❒ How many people live or work within one mile of your site: 500; 1,000; 2,000; 5,000; more than 5,000?

Section G - Security Environment & Overall Vulnerability to Attack

⇐ **Low** *Vulnerability*																			**High** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Does your organization have effective internal security procedures?
- ❒ What is the law enforcement presence in your area?
- ❒ What is the hardness, level of blast protection, etc. of your facilities?
- ❒ How accessible (security presence, access control, ID media, metal detection buffer zones, fences, etc.) is your facility?
- ❒ Are your assets and/or its potential recognized as a symbol?
- ❒ What level of public access is necessary for you to function?
- ❒ Can you control high-speed vehicle approaches to your facility?
- ❒ Do you have access control to your parking area?
- ❒ Do you conduct vehicle searches when entering facility grounds or parking areas?
- ❒ Do you employ detection/monitoring systems (video surveillance, intrusion detection systems, etc.)?
- ❒ Is your parking delivery area adjacent to or near your facility?
- ❒ Is your delivery area supervised during hours of normal business?
- ❒ Is your delivery area access blocked during hours that your business is closed?
- ❒ Do you have an on-site food service facility for employees and visitors?
- ❒ Is access to the water supply for your facility protected?
- ❒ Is access to the ventilation system for your facility protected?
- ❒ Do you have a way to quickly shut down the water supply or ventilation system for your facility?

Section H - How Critical are your Products of Services?

⇐ **Low** *Vulnerability*																			**High** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ What is the importance of your organization to the community?
- ❒ Is your organization critical to the local population, economy or government?
- ❒ Is your organization critical to the continuity of basic services?
- ❒ Is your organization critical to state or national commerce?
- ❒ What would be the social, economic or psychological ramifications of a terrorist attack against your organization?

- ❒ What is the nature of your assets: hazardous materials, uniqueness, potential danger to others, etc?
- ❒ How long would it take to restore your critical services/functions?

Section I - High Risk Personnel

⇐ **Low** *Vulnerability*																		**High** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Do you have personnel that are critical to the continuing function of State or local government, basic services, utilities infrastructure, the community, the economy, or of inherent value to your business or agency?
- ❒ Do you have personnel that are critical for responding to a terrorist act?
- ❒ What would be the effect of a terrorist act against these high risk personnel?

Section J - Organization Communications

⇐ **Low** *Vulnerability*																		**High** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Do you have a Mass Notification System (public address system, intercoms, and alarms)?
- ❒ Do you have a secure communications network that can be relied upon during a crisis?
- ❒ Do you have a crisis response team?
- ❒ Is your crisis response team trained?
- ❒ Do you conduct regular exercises?
- ❒ Do local/regional emergency responders participate in your exercises?
- ❒ Does your Crisis Response Team have its own portable communications system?
- ❒ Can your Crisis Response Team communicate directly with emergency responders?
- ❒ Do you have an emergency law enforcement notification system such as a hot line, panic button or something similar?
- ❒ Is your alarm system tied into the local law enforcement department or do you have an alarm service?
- ❒ Are your systems tested regularly?

Section K - Security and Response

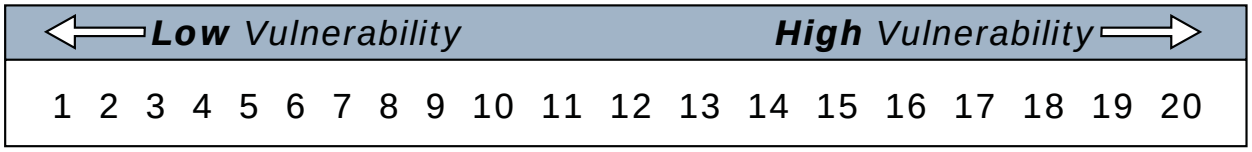
⇐ **Low** *Vulnerability*																		**High** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Are your security forces' staffing and training levels adequate?
- ❒ Do you have the capability to maintain a security presence in a high threat situation?
- ❒ Are additional security personnel available if requested?
- ❒ Are there affiliated agency/industry/organization support services available?
- ❒ Do you have trained disaster response teams within the organization?
- ❒ Do you have necessary specialty detection, monitoring, hazard assessment devices on hand and are they functional?

- ❒ Are local/regional law enforcement forces adequate and can they respond rapidly?
- ❒ Are local emergency responders familiar with your facility and its contents?
- ❒ Do you keep records on who visits your facility and where they go within the facility?

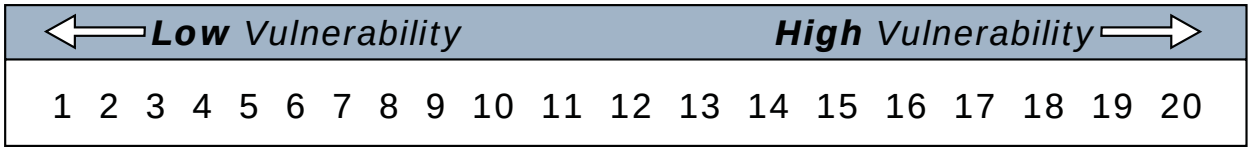
Section L - Policy/Procedures/Plans



Issues to be considered in selecting your score:

- ❒ Do you have a current crisis response/disaster plan?
- ❒ Does your plan include the types of crises you are most likely to encounter (e.g., fire, explosion, chemical release)?
- ❒ Are your employees familiar with the plan?
- ❒ Have you conducted crisis response and disaster drills and were they effective?
- ❒ Have you identified the critical functions of your workplace and do you have a plan for continuation of operation during an emergency?

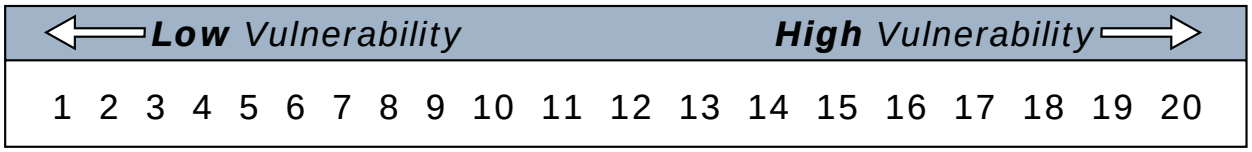
Section M - Security Equipment



Issues to be considered in selecting your score:

- ❒ Do you have a security system and is it current technology?
- ❒ Do you have an intrusion monitoring motion detector or an alarm system?
- ❒ Do your systems have back-up if power is cut or fails?
- ❒ Do you have security equipment that would detect leaks or ruptures of potentially hazardous materials?
- ❒ Do you have personnel protective equipment for your emergency response team appropriate for the hazardous materials at your facility?
- ❒ Is such equipment in working order and has it been inspected recently?

Section N - Computer Security - Cyber-Crime & Cyber-Terrorism



Issues to be considered in selecting your score:

- ❒ Is your site dependent on information technology such as computers and networks to accomplish its daily business activities?
- ❒ Is the information stored in your computer systems valuable?
- ❒ Do you have back-up power available for your computer systems?
- ❒ Do you make back-up copies of your data?
- ❒ Is your back-up data securely stored?
- ❒ Does your site have computers or networks connected to the Internet?

- ❒ Have you experienced problems with computer security incidents, such as computer viruses, worms, web-site defacements and/or denial of service attacks in the past?
- ❒ Do you have staff in place that are adequately trained and are available to monitor security warnings and take protective measures, such as loading system patches?
- ❒ Do you have technology security tools in place such as firewalls, intrusion detection systems or anti-virus software to protect your computer systems?
- ❒ Do you have a computer security policy, plan and procedure that includes a computer security incident response team?

Section O - Suspicious Mail And/Or Packages

⇐ **Low** *Vulnerability*																			**High** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Is the mail for your facility opened in a secured area or an area isolated from the majority of personnel?
- ❒ Have the personnel who open mail received training on the recognition of suspicious mail and/or packages?
- ❒ Do you have specific procedures on how to handle suspicious mail and/or packages, including possible facility evacuation?
- ❒ Do you have a secure and contained location where any unusual or suspect deliveries or mail can be stored until proper authorities can evaluate the suspect items?

Section P - Telephone, Bomb And Other Threats

⇐ **Low** *Vulnerability*																			**High** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Has your staff received training on how to handle bomb and other threat calls?
- ❒ Does your staff have a checklist of questions to ask the caller in case of a bomb or other threatening call?
- ❒ Does your facility have a plan on how to handle bomb and other threatening calls?
- ❒ Does your bomb threat plan include a system whereby your personnel would search your facility to identify suspicious objects to point out to emergency response personnel?
- ❒ Does your plan include a decision making process on whether to evacuate the facility?
- ❒ Are personnel familiar with the plan? Have evacuation drills been conducted?
- ❒ Is your plan coordinated with local law enforcement and the local phone company?

Section Q - Employee Health & the Potential for Bio-Terrorism

⇐ **Low** *Vulnerability*																			**High** *Vulnerability* ⇒
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Issues to be considered in selecting your score:

- ❒ Do you have an occupational health safety program in place?
- ❒ Do you have a health professional working at your facility?

- ❒ Do you have a procedure in place to track the health of each employee and know if more than one employee has the same symptoms?
- ❒ Do you monitor the health status of employees on sick status or absent otherwise?
- ❒ Are employees encouraged to keep supervisors informed on any unusual health related event or condition?
- ❒ Are employees required to report any unusual conditions or substances encountered in the course of their normal duties, such as strange substances or odors from packaging or mail?
- ❒ Do employees know the proper procedures for emergency operation or shut-off of air handler, air circulating or ventilation systems?
- ❒ Do you keep a current list of employees, home addresses and emergency contact information?
- ❒ Do you have an emergency notification plan for employees (e.g. calling tree)?

Total Score: _____

Self-Assessment Evaluation:

20 -------Low Risk --------85

86--------Low Caution---170

171------High Caution---255

256------High Risk--------340

If the total score for the transportation organization exceeds 256, and if local law enforcement has not been involved in the assessment, then the airport should notify the FBI and local law enforcement and provide them with copies of the assessment worksheet.

Remarks/Unusual or Significant Issues:

Please list any important remarks you think should be made concerning your self-assessment. Also, please list any unusual or significant findings that you developed during your self-assessment, list significant hazardous materials that might be used as a terrorist weapon or any significant impact a terrorist act against your site may cause to the community.

_____

_____

_____

_____

_____

_____

Attach additional sheets if necessary.

APPENDIX B

AIRPORT SECURITY SPACE PLANNING

Section A - Introduction

This Appendix provides general methodology, equations and information used to determine the approximate number, size and configuration of space required for security screening checkpoints. These are generic formulas based on time-tested airport industry security flow modeling experience. While they will not necessarily provide a final design solution, they are an excellent tool for determining the space planning requirements in the initial planning phases of new or modified construction. Refer to the *Security Screening* section on page 87 for further information.

Section B - Space Planning Aids

This section presents calculations used to determine the number, size and configuration of required SSCPs.

- Growth factors for anticipated future increases in traffic and the accompanying increases in expanded terminal space should also be considered by the planner, bearing in mind that there are typically several years lag time between conceptual terminal design and actual construction, and that FAA estimates between 3%-5% *annual* passenger growth.
- The planner's calculations must also adjust estimates of peak hour volumes for situations where split operations, multiterminal operations and multiple SSCP may serve to distribute peaks, either evenly or unevenly, throughout various terminals and/or concourses.
- Similar calculations and formulas are used by International Air Transport Association (IATA) and planners in the United Kingdom's Department of Transport document "Aviation Security in Airport Development".

1. Planning Passenger Volume

Airports experience very large variations in demand levels over time which can be described in terms of:

- Annual variation over time
- Monthly peaks within a particular year
- Daily peaks within a particular month or week
- Hourly peaks within a particular day

Many airport terminals are busy for various time segments in a day, and have no traffic for some other periods during the day. In order to determine the number of SSCPs, annual or daily demand does not provide sufficient information. There is a need to capture the levels of demand on the SSCPs for the peak periods during the planning day. However, the choice of the planning day is important. It is not advisable to select the planning day as the busiest day of the entire year since that will oversize the facility, resulting in underutilization and high design and building costs.

One commonly used technique is to identify a peak hour for which the facility is to be designed and compute the total passenger volume for that period. The peak hour volumes typically range from 10% to 20% of the daily volume. There are several methods to determine the design load on the SSCPs, and the list below identifies four methods1:

a. Typical Peak Hour Passengers (TPHP)

b. Busy Day/ Peak Hour (BDPH)

c. Standard Busy Rate (SBR)

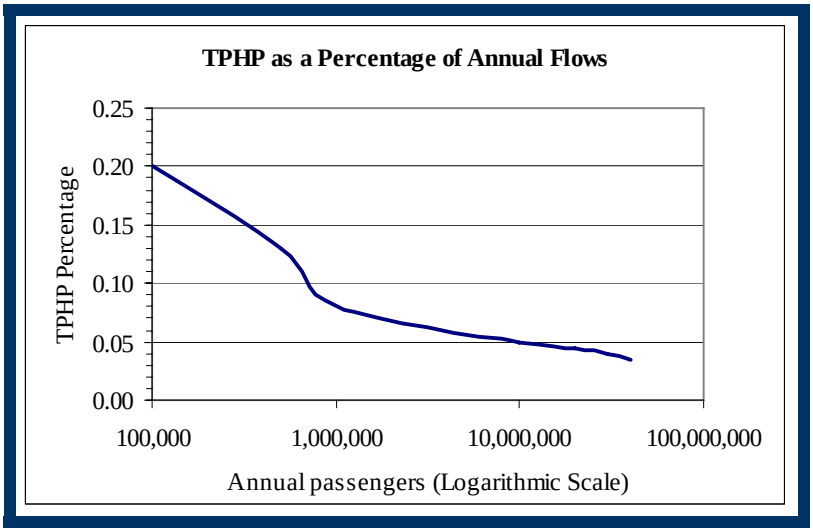
d. Busy Hour Rate (BHR)

[1] Ashford, Norman, H. P. Martin Stanton and Clifton A. Moore, Airport Operations, 2nd edition, McGraw-Hill, 1997.

a. Typical Peak Hour Passengers (TPHP)

The planning day is suggested to be the Average Day of the Peak Month (ADPM). ADPM represents the most common method of converting planning statistics to a daily and ultimately to an hourly demand baseline2. The determination of ADPM requires the identification of the peak month for the facility under consideration. Most common peak months are July and August. The next step is to identify an average day demand profile for the peak month. This is typically calculated by dividing the peak month demand by the number of days in the peak month.

The Typical Peak Hour Passengers denote the number of passengers for the peak hour of the planning day (ADPM). The peak hour in a planning day can be calculated based on the actual flight schedule for the ADPM. Typically, large airports have peak hour volume of 10 to 20 percent of the daily volume. As seen in this figure, the peak is more pronounced for smaller airports, and as airports grow larger, the peaks flatten since there are departures and arrivals scheduled throughout the day. For SSCP design purposes, only the annual departures (enplanements) should be considered in the peak hour volume. If the annual volume includes both arriving and departing passengers, one can assume that half of the total volume accounts for the departing passengers. Greeters, family, etc., are accommodated in the formulas.



Appendix B Figure B-1 - Recommended Relationship for TPHP Computations from Annual Figures

b. Busy Day/Peak Hour (BDPH)

IATA suggests the BDPH method for design and planning purposes. The "busy" day is defined as the second busiest day in an average week during a peak month. An average weekly pattern of passenger traffic is calculated for that month. Peaks associated with special times such as national holidays, festivals, fairs, special events are excluded. The busy day data can be obtained from the airport tower log. Once the aircraft movements are obtained, passenger volumes can be plotted by time-of-day with appropriate load factor assumptions. This will lead to the selection of peak hour and corresponding passenger volume within that 60-minute period. The detailed security checkpoint planning will then be based upon the busy hour passenger volume.3

Take care that calculations are not skewed by airline scheduling anomalies, such as the common practice of multiple airlines scheduling their first flight of the day at 6:59 a.m. or 7:59 a.m. in order to be the first one listed in the reservations computers.

[2] USDOT – FAA Advisory Circular. Planning and Design Guidelines for Airport Terminal Facilities, 4/22/1988.
[3] IATA, Airport Development Reference Manual, 8th edition, 1995.

c. Standard Busy Rate (SBR)

The Standard Busy Rate measure is mostly used in Europe. It is defined as the anticipated level of demand during a busy hour. For example, some European airports use 30th busiest hour of passenger flow for the entire year. SBR demand in practice is very similar to that of TPHP. The IATA recommends that the extraordinarily high-traffic seen for major holidays be excluded in selecting busy periods.4

d. Busy Hour Rate (BHR)

The BHR is a variation of the SBR where the volume is estimated by the rate above which 5 percent of the traffic at the airport is handled. It is computed by ranking the hourly operational volumes for the entire year, and then selecting the hourly volume for which 5% of all hourly volumes is exceeded.

There are other lesser-used techniques utilized to compute the peak volume; namely Busiest Timetable Hour, Peak Profile Hour, and several other variations.

2. Calculations

The calculations presented in this section should be used as a general guideline to determine the number of SSCPs. In order to estimate the number of required SSCPs, the following parameters need to be defined first.

a. Demand Parameters

P	=	Planning hour passenger enplanement volume. (People per hour)
T	=	Percentage of transfer passengers that bypass screening. E.g., 0.2 represents 20% of passengers connecting within the secured area, who thus need not go through screening.
K	=	A percentage of originating passengers to represent meeters/greeters, well-wishers, employees, and vendors using the SSCPs.
r	=	Demand scale factor between 1 and 1.4 to account for variability of arrival rate through the planning hour.
L	=	Effective demand on the SSCP. (Includes passengers, meeters/ greeters, well-wishers, and airport employees.)

b. SSCP Parameters

S	=	Service rate of the SSCP. (People per hour)
f	=	SSCP utilization factor. Typically between 0.80 and 0.95. This multiplier represents the utilization factor for both the equipment and staff. It is essential in the design that the equipment and staff is not designed to operate on full capacity. This factor accounts for equipment breakdowns, staffing fluctuations, and other disruptions in the process.
X	=	X-ray belt service rate. (Bags per hour)
B	=	Number of carry-on bags per passenger.

The effective hourly load on the SSCPs is a function of the peak hour enplanements, the transfer percentages within the secured area, other traffic such as the meeters/greeters, well wishers, employees and vendors represented as a percentage of enplanements, as well as the demand scale factor *r*.

$$L = P * (1 - T) * (1 + k) * r \qquad \textbf{Equation 1}$$

The demand scale factor r plays an important role in determining the "true" peak load on the SSCPs.

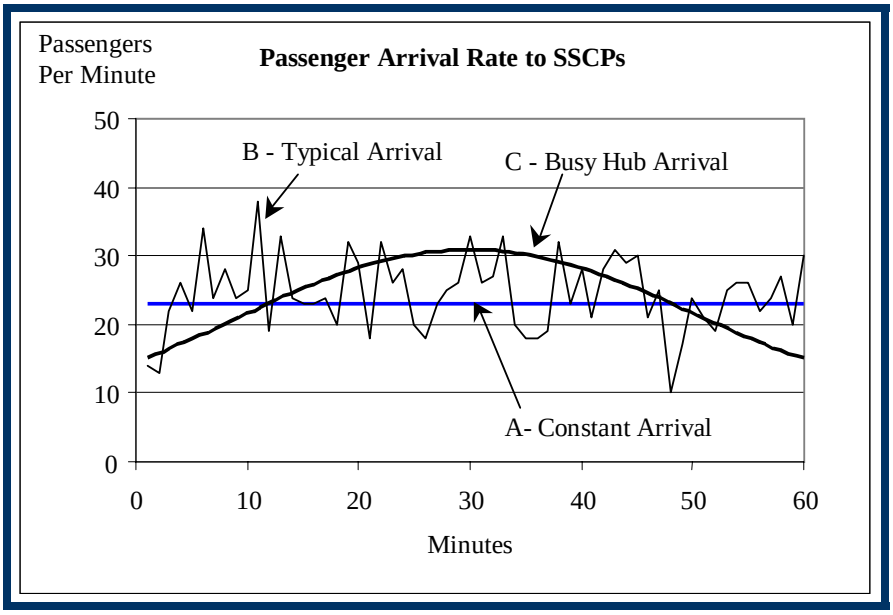
Consider the following example. Assume a peak flow of P=1,600 enplaning passengers per hour, with T=25% of passengers transferring within the secured area and other traffic (meeters/greeters, well wishers,

[4] Measuring Airport Landside Capacity, Transportation Research Board, National Research Council, Spec. Report 215, Washington, D.C., 1987.

employees and vendors) accounting for k=15% of enplaning passengers. With a demand scale factor of *r*=1, the effective hourly load on the SSCP is:

$$L = 1{,}600 * (1 - 0.25) * (1 + 0.15) * 1.0 = 1{,}600 * 0.75 * 1.15 * 1.0 = 1{,}380$$

In this example, L=1,380 indicates a constant arrival pattern where people arrive to the SSCP with 1,380/60=23 people per minute. However, this will not be the case in many airports. The figure below shows three different arrival patterns, all of which have the same arrival rate of 1,380 passengers per hour.



Appendix B Figure B-2 - Different Arrival Rates to SSCPs - All Cases with 1,380 passengers per hour

Case A assumes a constant arrival pattern where arriving passengers are spread uniformly. This results in a constant demand on the SSCPs with 23 passengers per minute.

Case B is more realistic by assuming random arrivals where the per minute rate changes between 10 to 40 passengers per minute, with the same total of 1,380 passengers arriving in an hour.

Case C also has variation in the number of passengers arriving per minute, but also with a total of 1,380 passengers arriving in an hour. However, in this case, the arrivals peak in the middle of the peak hour.

c. The Effect of Demand Scale Factor *r*

The demand scale factor *r* is used to represent the effective demand on the SSCPs. This quantity typically ranges from 1.0 to 1.5 depending on the variation in the arrival process.

Case A - Constant Arrival – No Variation

In this case, the demand scale factor *r* can be set to 1.0. Case A in the Figure represents this. This case is not very realistic since passengers do not arrive at the SSCP in a constant flow or pattern.

Case B - Typical Arrival – Medium Variation

This case represents medium variation in the demand, and is seen in main SSCPs used by originating passengers in medium-scale airports. In this scenario, the arrival rate is metered by the ticketing operation. This case presents more load on the SSCPs due to randomness in the arrival pattern, thus warrants the use of larger *r*, possibly between 1.0 to 1.2. Case B in the Figure represents this.

Case C - Busy Hub – High Variation

This is a typical arrival patterns for hub operations during busy bank departures. This case warrants for the use of large *r*, possibly between 1.1 and 1.4. Case C in the Figure represents this. The choice of large *r* is also warranted for large transfer operations that require security processing.

3. Number of Checkpoints – Centralized (General Configuration)

This section presents general formulas and calculations for determining the number of checkpoints for a centralized SSCP.

a. Required parameters

P	=	Peak hour enplanements
T	=	Transfer percentage
k	=	Percentage of enplaning passengers to account for other airport traffic
r	=	Demand scale factor between 1 and 1.5
f	=	SSCP utilization factor
S	=	SSCP service rate in people per hour

b. Number of Checkpoints

The formula shown below can be used to determine the required number of checkpoint stations:

$$N_{checkpoints} = \frac{P*(1-T)*(1+k)*r}{S*f} \qquad \textbf{Equation 2}$$

c. Example

P	=	1,600 passenger per peak hour.
T	=	25% of passengers transferring within the secured area.
k	=	15% of enplaning passengers to account for other traffic (meeters/greeter, well wishers, employees and vendors.)
r	=	Demand scale factor of 1.2 to account for randomness in arrival pattern.
f	=	80%
S	=	600 people per hour.

$$N_{checkponts(r=1.2)} = \frac{1{,}380*1.2}{600*0.8} = 3.45 = 4$$

In this example, the demand scale factor of *r*=1.2 dictates 4 screening stations. To facilitate the discussion on the effect of *r*, let's assume that the facility serves a uniform demand, thus *r*=1. Under this scenario, the total number of required screening checkpoints is calculated as:

$$N_{checkpoints(r=1)} = \frac{1{,}380*1.0}{600*0.8} = 2.875 = 3$$

This example shows the importance of demand pattern throughout the peak hour. If arrivals throughout the peak hour can be assumed to follow a uniform pattern, than *r* should be set to 1. However, arrivals follow a bell-curve shape throughout the peak hour, thus setting *r* to 1.2 is more realistic.

4. Number of Checkpoints – Centralized (X-Ray + Metal Detector)

In this common SSCP setup, a combination of x-ray belt and metal detector is used to check baggage and passenger, respectively.

a. Required parameters

P	=	Peak hour enplanements
T	=	Transfer percentage
k	=	Percentage of enplaning passengers to account for other airport traffic
r	=	Demand scale factor between 1 and 1.5
f	=	SSCP utilization factor
X	=	X-ray belt service rate in bags per hour
B	=	Number of carry on bags per passenger

b. Number of Checkpoints

The required number of x-ray processing stations is:

$$N_{x-ray} = \frac{P*(1-T)*(1+k)*r*B}{X*f}$$

c. Example

P	=	1,200 passengers per hour
T	=	50% of passengers transferring within the secured area
k	=	15% of enplaning passengers to account for other traffic (meeters/greeter, well wishers, employees and vendors.)
r	=	Demand scale factor of 1.2
f	=	SSCP utilization factor of 0.9
X	=	700 bags per hour
B	=	An average of 1.5 bags per passenger

$$N_{x-ray} = \frac{1{,}200*(1-0.50)*(1+0.15)*1.5*1.2}{700*0.9} = 1.97 = 2$$

This formula results in 2 x-ray devices, which could be served by a common metal detector, and a secondary manual search station staffed accordingly.

5. Number of Checkpoints – Holdroom (X-Ray + Metal Detector)

This section presents security checkpoint sizing formulas where SSCPs are placed at the entrance of the holdroom. In this scenario, the terminal concourse is not secured, and passengers clear security only at the gate holdroom. It is assumed that a combination of x-ray belt and metal detector is used to check baggage and passenger, respectively.

a. Required parameters

M	=	Maximum number of passengers on a departing flight handled at the gate holdroom.
T	=	Transfer/through percentage
k	=	Percentage of enplaning passengers to account for other airport traffic
r	=	Demand scale factor between 1 and 1.5
f	=	SSCP utilization factor
X	=	X-ray belt service rate in bags per hour

B = Number of carry on bags per passenger

G = Duration of time (in minutes) that holdroom is open. This is typically reflected by the difference between the time of arrival of the first passenger to the holdroom and the time when the last passenger is on board.

b. Number of Checkpoints

The required number of x-ray processing stations is:

$$N_{x-ray} = \frac{M * (1-T) * (1+k) * r * B}{X * f * (G/60)}$$

c. Example

M = 340 passengers

T = 10% (The percentage of through passengers that remain on board)

k = 0% (Only passengers holding boarding ticket/cards are allowed in the holdroom)

r = Demand scale factor of 1.2

f = SSCP utilization factor of 0.9

X = 800 bags per hour

B = An average of 1.5 bags per passenger

G = The gate is open for 50 minutes prior to the departure

$$N_{x-ray} = \frac{340 * (1-0.10) * (1+0) * 1.5 * 1.2}{800 * 0.9 * (50/60)} = 0.918 = 1$$

The formula results in 1 x-ray device, which can be served by a metal detector and a secondary manual search station.

When the holdroom serves more than one gate with simultaneous departures, the parameter M needs to be adjusted to represent the sum of all passengers leaving the holdroom in an hour.

6. Queue Size

The space needed for queuing in front of the SSCP and the amount of time passengers wait to be processed are both dependent upon the SSCP processing rates. The higher the processing capacity, the queues and wait times will be shorter. In designing the space around the SSCP, one often targets a maximum waiting time tolerable by individuals. This time is typically in the magnitude of 2 to 8 minutes. There is a theoretical queuing rule known as Little's Result that shows that the average number waiting in the queue is a product of the arrival rate and the average waiting time in the queue.5 Using this result, the equation below gives the necessary queue size.

a. Required parameters

P = Peak hour enplanements

T = Transfer percentage

k = Percentage of enplaning passengers to account for other airport traffic

W_{target} = The target maximum wait time in the queue. Typically between 2 to 8 minutes.

r = Demand scale factor between 1 and 1.5

[5] Kleinrock, Leonard, Queuing Systems, Volume II: Computer Applications, John Wiley & Sons, 1976.

The effective demand on the SSCP is denoted by L and is described below.

$$L_{minutes} = \frac{P*(1-T)*(1+k)*r}{60}$$

The number of people waiting to be serviced by the SSCPs can be expressed as:

$$Q_N = L_{minutes} * W_{target}$$

b. Example

Let's consider the example provided earlier that required 2 x-ray processors:

P	=	1,200 passengers per hour
T	=	50% of passengers transferring within the secured area
k	=	15% of enplaning passengers to account for other traffic (meeters/greeter, well wishers, employees and vendors.)
r	=	Demand scale factor of 1.2
W_{target}	=	Tolerable wait time of 5 minutes

The effective demand per minute is given by L:

$$L_{minutes} = \frac{1{,}200*(1-0.5)*(1+0.15)*1.2}{60} = 13.8$$

With target maximum waiting time of W_{target}=5, the number of people expected to queue in front of the SSCP is given by Q_N:

$$Q_N = 13.8*5 = 69$$

With two x-ray machines, there will be two queues each with approximately 35 passengers.

APPENDIX C

AIRPORT BLAST PROTECTION

Section A - Introduction

The Department of Homeland Security (DHS), Transportation Security Administration (TSA), and Federal Aviation Administration (FAA) have deemed that it is important to provide some measure of "blast" protection to passengers, personnel, and facilities at airports from "Improvised Explosive Devices" (IED) and "Large Vehicle Improvised Explosive Devices" (LVIED). The impetus to protect passengers and personnel at airports has led to a succession of mandated security directives. Many of these security mandates have greatly affected how airports operate during heightened threat levels (orange and red) and have impacted airport revenues significantly. Thus it has become increasingly important to consider how best to plan and design airport terminals, roadways, and essential ancillary facilities with blast protective measures in mind.

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 readily adapts 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.

1. Why Airports?

There are countless potential terrorist targets worldwide. Targets range from certain building or businesses to specific social, religious, and political groups. Transportation facilities such as airports, subways, train stations, and bus stations are all potential targets of terrorism. Unfortunately, this fact has been proven around the world over the past several years. Airports are targeted because they are:

- Vital to a stable economy.
- Important to the operation of countless businesses.
- Filled with a high density of people.
- Very visible, high-profile facilities.

Therefore, not only has the TSA mandated some measure of blast protection at airports, it is also apparent that providing some deterrents and protection against potential terrorist attacks is a prudent thing to do.

2. Risk Management

Protection from IED and LVIED threats can be provided in many forms:

- Mobile Security: security personnel, K-9 units, cameras, sensors, alarms, etc.
- Standoff: separation between a potential bomb source and the target.
- Physical Protection: gates, barriers, blast-hardened columns, blast debris screens, blast-resistant windows, etc.
- Risk Acceptance: prioritization of protective measures based upon a vulnerability assessment, implementation cost, and overall airport security plan.
- Blend of All of the Above: 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 mitigate all potential LVIED 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, some amount of "risk acceptance" is necessary. In other words, the public has grown accustomed to driving on the interstate freeway at 70 miles per hour; yet, without some measure of risk

acceptance in doing so, the speed limit would need to be adjusted to around 10 miles per hour and automobiles would need to be built with substantially more crash restraints, cushions, and bumpers—none of which would be practical or cost effective. 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, and be unacceptable to the traveling public. Therefore, each unique airport is left with making important decisions on how best to provide security and blast protection while weighing the effectiveness, cost, and impact to airport operations.

3. Planning Facility Blast Protection

Security planning must be an integral part of all projects undertaken at an airport. Security planning should include:

- Performing periodic vulnerability assessments of all facilities and the airport site.
- Evaluating the existing security program to confirm that federal, state, and local standards have been met.
- Training and informing employees, contractors, and consultants with the latest security procedures and issues.
- Defining procedures that summarize actions and responsibilities in the event of an emergency (natural or manmade).
- Reviewing the plans and layout of new facilities in light of the latest TSA and DHS security mandates and new security technologies.

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 emphasis and highest 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 terrorist bombing occurs. In other words, the loss of life due to a terrorist bombing reduces significantly if the building remains standing and does not collapse. As such, preventing the building from collapsing is a very high priority.

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 safely and effectively—even during high threat levels. Furthermore, incorporating "blast resistant" features during the initial design costs little and blends with the overall building architecture much better than retrofitting a facility after the fact.

Unfortunately, most airports were designed several years ago with very different security needs and criteria in mind. As a result, the opportunities for providing a blast-resistant facility are often limited to mobile security.

It is significant that airport personnel and tenants understand a clear delegation of airport security responsibility. In addition, a plan should be in place that addresses the chain of command and modifications to airport operations during emergencies such as those caused by nature, accidents, fire, terrorism, and sabotage.

Section B - Common Airport Blast Protection Issues

The following is a summary of common vulnerability issues and recommended methods to physically harden or protect airport facilities. The suggested security enhancements are not mandatory. Rather, they 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 inherently allow thousands of people and vehicles that have not been screened for weapons or explosives to be in close proximity to the facilities. However, with a certain amount of thought and planning, one can identify vulnerable areas and identify options to mitigate those threats.

1. Level of Blast Protection

In general, the objective for protecting airports is to provide a “medium" level of blast protection. A medium level of protection recognizes 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.

2. Common Vulnerabilities

a. Roadways

- The roadways that surround airport terminals are designed to allow convenient passenger access. Unfortunately, passenger convenience is often contrary to good security planning. Vehicles that enter airport "landside" property typically are not inspected, weighed, or screened except during high threat levels (as defined by the TSA). Restricting or monitoring vehicles that enter landside areas of the airport sounds unusual. However, other "secure" buildings, i.e., courthouses and embassy buildings, would not allow unrestricted or uninspected access. Furthermore, 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.
- Many airports have multi-level roadways (refer to *Appendix C Figure B-1* below) 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 LVIED attacks.

Appendix C Figure B-1 - Elevated Roadway

- 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 *Appendix C Figure B-2* and *Appendix C Figure B-3* below).

Appendix C Figure B-2 - Curbside Drop-Off at Ticketing Level

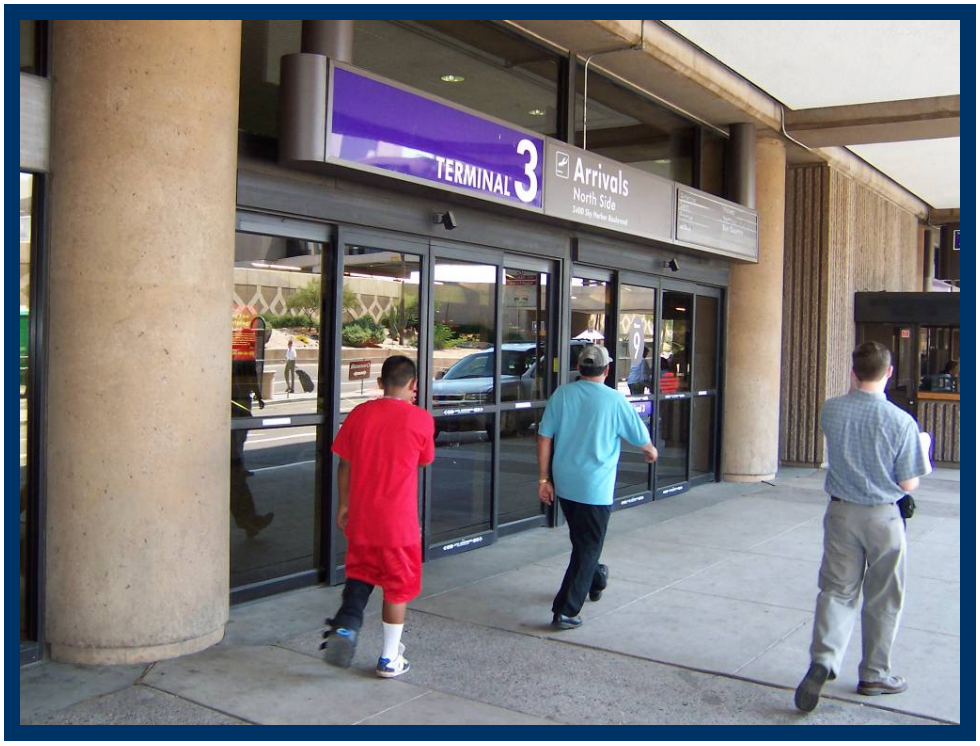
Appendix C Figure B-3 - Curbside Pickup at Baggage Claim Level

b. Terminal Perimeter

- The exterior windows and doors often 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 terrorists that are able to flank around the hardened façade simply by walking through the entry doors with unscreened luggage in tow.
- 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 *Appendix C Figure B-4* below for an example of column hardening by wrapping process.

Appendix C Figure B-4 - Wrapping Process - Kevlar-Carbon Fiber Wrap

- Many large vehicles often 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 away in these vehicles, and since they are very difficult to visually inspect, they virtually have open access to deliver their bulk threat to any part of an airport.
- The exterior doors often are not protected from vehicular attack (refer to *Appendix C Figure B-5* below).



Appendix C Figure B-5 - Exterior Doors

- The exterior trash containers and mail receptacles (refer to *Appendix C Figure B-6* below) 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. 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.

Appendix C Figure B-6 - Trash Container

- There often are areas at curbside, such as luggage counters, that could conceal explosive devices (refer to *Appendix C Figure B-7* below). Areas that allow for explosive devices to be hidden should be avoided. This includes benches, booths, planters, landscaping, etc. Avoid landscaping and furniture that permits concealment of criminals or obstructs the view of security personnel or closed-circuit television.

Appendix C Figure B-7 - Potential Concealment Area at Ticketing Level

c. Terminal Landside

- Passenger baggage presents an unusual challenge. While people carrying large, heavy bags might seem unusual in most situations, it is quite common in an airport environment. Therefore it affords a potential bomber the opportunity to reasonably carry up to 75 pounds or more of explosives inside a terminal without much scrutiny—especially in terminals that service international flights, where passengers consistently travel with oversized luggage. In addition, baggage claim areas offer a prime target of opportunity in those 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.
- 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.
- Loading docks and shipping/receiving areas oftentimes are not 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 *Appendix C Figure B-8* below), the airport should consider hardening the area to resist bomb blasts, and the room should be "vented" outward.

Appendix C Figure B-8 - Loading Dock

- 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 must be performed to justify parking within 300 feet of the terminal during orange or red threat levels.

d. Fuel Facility

- The fuel farms that service the airport often can be vulnerable. For example, there may be an uncontrolled parking lot that is not owned by the airport which is adjacent to the fuel facility. The proximity to public perimeter parking or roadways makes the fuel facility vulnerable (refer to *Appendix C Figure B 9* below.

(a) Adjacent Parking Lot **(b) Adjacent Roadway**

Appendix C Figure B-9 - Fuel Facility

e. Power Substation

- The main power for the airport complex should be provided with redundant power and emergency power. Avoid placing substations adjacent to public roadways.

f. Air Traffic Control Tower

- The ICBO UBC defines Air Traffic Control Towers (ATCT) (refer to *Appendix C Figure B-10* below) as essential facilities. Obviously, the airport must have a fully functional ATCT in order to operate. Pubic 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.

Appendix C Figure B-10 - Air Traffic Control Tower

3. 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, including fuel systems, day tank, fire sprinkler, and water supply
- Fuel storage and fuel delivery systems for aircraft
- Main switchgear
- Telephone distribution and main switchgear
- Fire pumps
- Building security control centers
- UPS systems controlling critical functions
- Main refrigeration systems that are critical to building operations
- Elevator machinery and controls
- Shafts for stairs, elevators, and utilities
- Critical distribution feeders for emergency power
- Navigational and communications equipment
- Airport Emergency Command Post
- Electrical substations (local and regional)

Section C - 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 effectiveness. 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 to ensure that implementation of these measures do not result in downstream consequences that create a more hazardous situation.

1. Blast-Protection Protocols

a. Blast Envelope

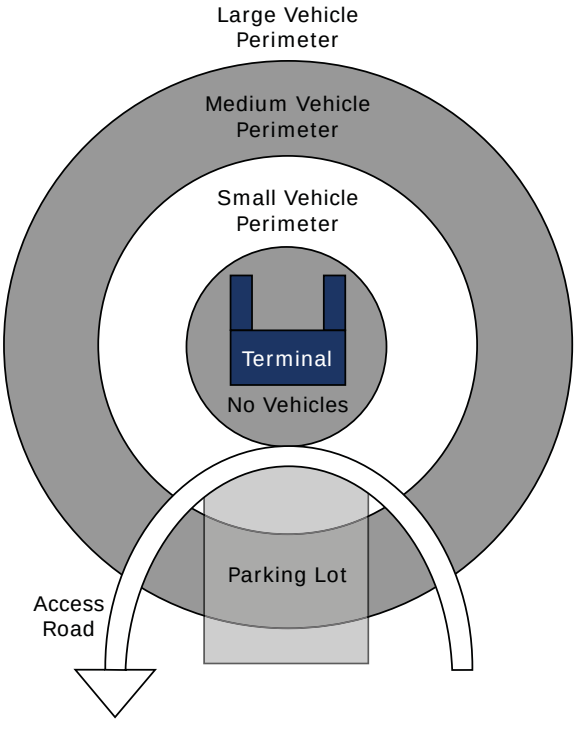
Typical security protocols involve the establishment of security perimeters, or rings, that act as filters to keep potential threats from their targets. In this case, during higher threat potential, vehicle restriction would be imposed by the TSA to keep LVIEDs from the terminal. This system of rings can manifest itself in many ways.

A blast analysis will need to be performed in order 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 (BATF) have identified some basic vehicle sizes and explosive carrying capacities:

Appendix C Table C-1 - Examples of Vehicle Explosives Capacity

Explosives Capacity	Vehicle Type	Examples
500 pounds	Compact Sedan	Ford Escort, Chevy Cavalier
1,000 pounds	Small/Medium SUV	Chevy Blazer, Ford Explorer
1,000 pounds	Full-Size Sedan	Ford Taurus, Chevy Impala
1,000 pounds	Small Pick-up	Nissan, Toyota, Ford Ranger, Chevy S-10
2,000 pounds	Large Pick-up	Full-Size Chevy, Ford, Dodge
2,000 pounds	Large SUV	Chevy Suburban, Chevy Tahoe, Ford Expedition
4,000 pounds	Large Cargo Van	Ford Club Wagon

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 *Appendix C Figure C-1* below).



Appendix C Figure C-1 - Blast Envelope

b. 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 LVIED 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 bypass routes, but rather only routes to lead vehicles away from the inspection area. For example, such routes might take vehicles 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.

c. Mobile Patrols

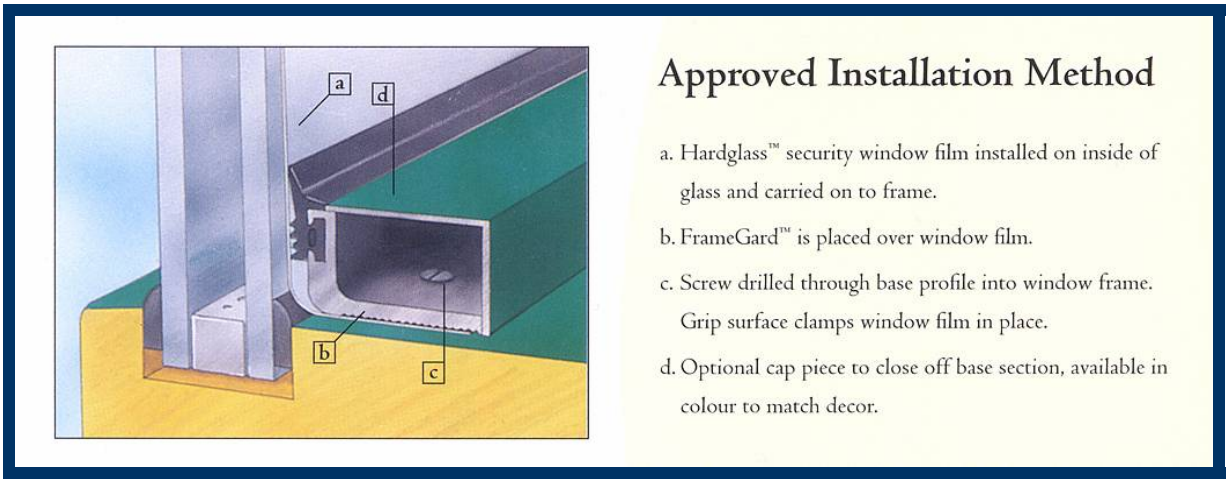
In addition to physical enhancements, mobile patrols can provide a significant deterrent especially when they are coupled with canine patrols. Patrols will need to watch curbside vehicle activity to spot any unusual driving behavior, as well as passengers and personnel inside the terminal. Canine patrols can be used throughout the airport environment as a means to detect possible explosive devices or vehicles. It is important to note that canines are used as a means to detect explosives, not to "clear" IEDs. Once someone or something is suspected of having or being an IED, only the responding bomb squad can actually clear the device or determine its safety. Simply because a canine does not react to a suspect package does not make that package safe to open or move. In some cases the canine simply cannot smell the threat.

2. 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 various components. In addition, some limitations of these hardening techniques also are listed. Although much blast testing has been performed, additional blast testing is ongoing by various agencies.

a. 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.

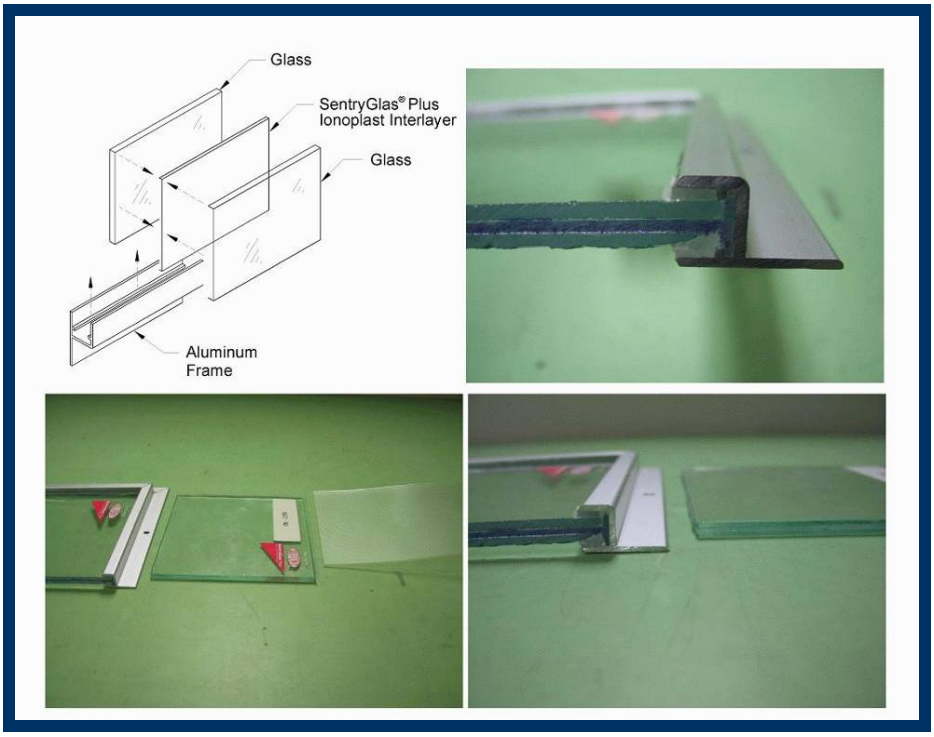


Appendix C Figure C-2 - FrameGuard™ Installation Method

Limitations: When the design blast pressure is exceeded, large "panels" of the hardened windows tend to fail. These window panels can be lethal. Therefore, 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 (refer to *Appendix C Figure C-2* above). A mock-up of an in-situ window panel should be performed prior to implementing this material. Window film has a limited lifespan, especially in direct sunlight. Window film can be scratched.

b. Conventional Window Replacement

Current "state-of-the-art" window replacement systems show that replacement windows can resist peak blast pressures of approximately 10 to 20 pounds per square inch (psi). Blast-resistant window systems should be laminated thermally tempered, laminated heat strengthened, or laminated annealed glass (refer to *Appendix C Figure C-3* below). 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.



Appendix C Figure C-3 - Conventional Window Replacement System

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.

c. High-Energy Absorbing Window Systems

Finite Element 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 (refer to *Appendix C Figure C-4* below) shows a successful blast test of a 'high energy-absorbing cable-supported curtain wall glazing system'.

Appendix C Figure C-4 - High Energy-Absorbing Cable-Supported Curtain Wall Glazing System

d. Column Wrap

Kevlar and carbon fiber wraps (refer to *Appendix C Figure C-5* below) can substantially improve the blast resistance of reinforced concrete columns. These systems have been installed in several retrofit conditions.

Appendix C Figure C-5 - Column Wrapping Procedure

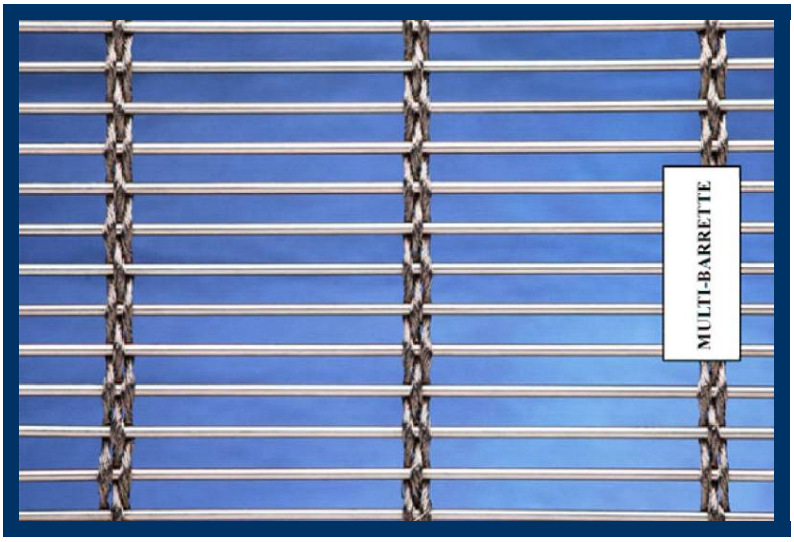
Limitation: The column wrap will affect the visual surface finish and texture of the columns.

e. Column Steel Jackets

Steel jackets can substantially improve the blast resistance of reinforced concrete columns. These systems have been installed in several retrofit conditions.

f. Stainless Steel Curtains (Catcher System)

Stainless steel curtains have been successfully blast tested as a "catcher" system (refer to *Appendix C Figure C-6* below) for medium-size IEDs.



Appendix C Figure C-6 - Close-up View of Metal Fabric Catcher System

g. Polyurethane/Polyurea Elastomer Coating (LineX)

Blast tests of 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.

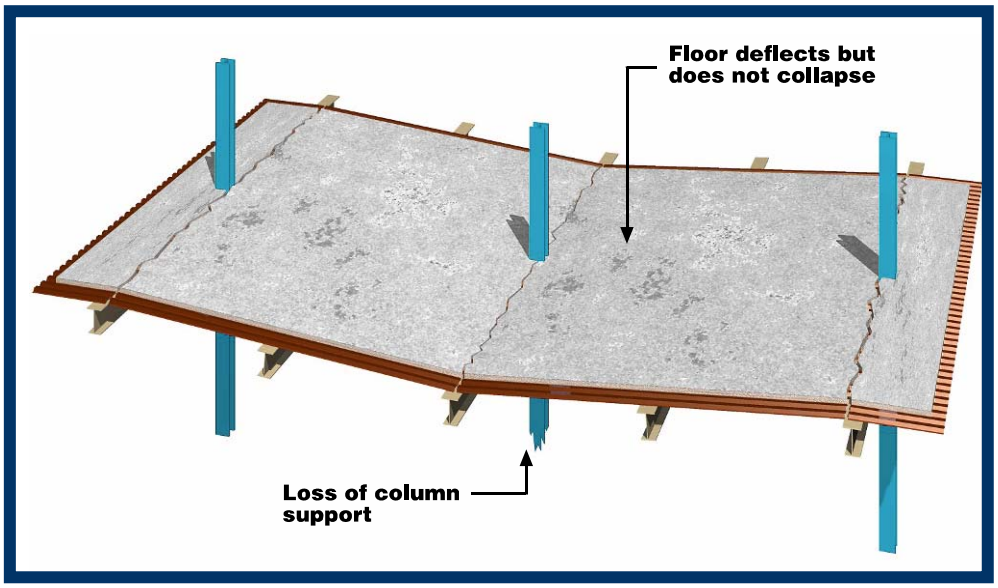
h. Composite Wall of Steel-Plated Walls

Testing and analysis has shown that a composite wall system (refer to *Appendix C Figure C-7* below) can provide blast and ballistic protection from LVIED size bombs at close proximity.

Appendix C Figure C-7 - Composite Wall of Steel-Plated Walls

i. 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" (refer to *Appendix C Figure C-8* below).



Appendix C Figure C-8 - Catenary Cable Floor Support System

Limitation: Corner columns cannot be protected in this manner, and this system does not prevent slab or girder breaches from explosions.

j. 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 *Appendix C Figure C-9* below) and elevated structures.

Appendix C Figure C-9 - Vehicle Barrier for At-Grade Condition

Limitations: Aesthetic and operational issues should be considered prior to implementing vehicle barriers. Operational issues resulting from narrowed roadways, including fire truck and emergency vehicle access, must be considered prior to implementing vehicle barriers.

k. 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 and around 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 *Appendix C Figure C-10* on page C-21 and *Appendix C Figure C-11* on page C-22). Another option is to use dual-plate composite blast walls for this protection.

l. **Threat Containment Vessel**

Proprietary Threat Containment Vessels (TCV) are available to resist improvised explosive devices of various sizes. A vessel capable of resisting a 50-pound TNT charge would suit most airport applications (refer to *Appendix C Figure C-10* below). Some models can contain chemical and biological gasses as well.

Appendix C Figure C-10 - Large IED Threat Containment Vessel

m. Mobile Threat Containment Unit

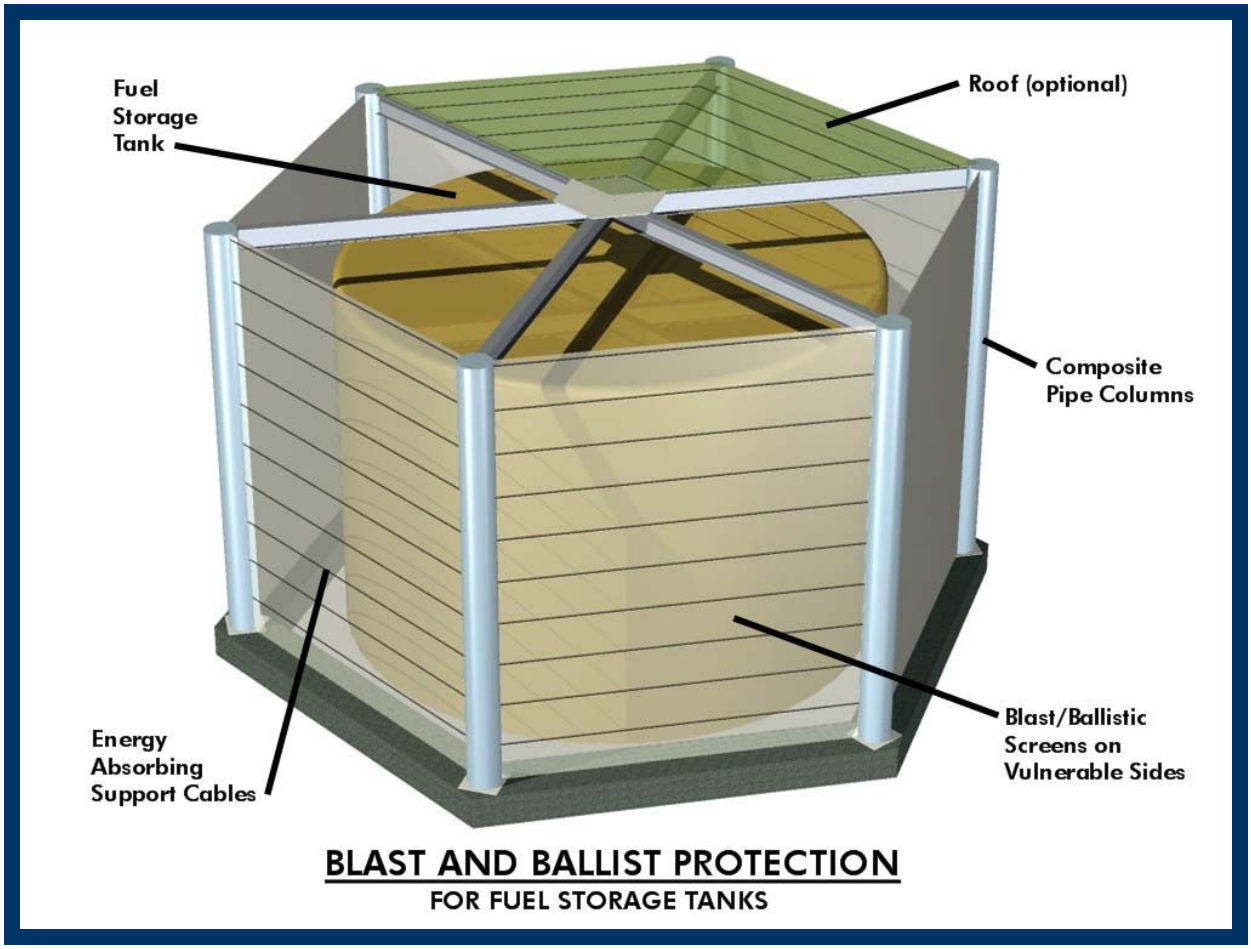
A mobile Threat Containment Unit (TCU) (refer to *Appendix C Figure C-11* below) is capable of providing safe storage of small IEDs (7 pounds of TNT).

Appendix C Figure C-11 - Small IED Threat Containment Unit

Limitation: The portable TCU cannot contain chemical and biological agents when dispersed with explosives.

n. Fuel Storage Tank Protective Screen

To protect fuel tanks, substations, etc., a blast/ballistic screen assembly (refer to *Appendix C Figure C-12* below) 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). Composite columns have excellent blast-resistance and strength properties.



Appendix C Figure C-12 - Blast and Ballistic Screen Assembly for Fuel Storage Tanks

Section D - Explosives Security Survey

It is beneficial to perform an Explosives Security Survey during the design of an airport and periodically after the airport has been built. An explosives security survey will assist in identifying areas and components of the airport that are vulnerable to acts of terrorism or sabotage.

Section E - Blast Analysis Tools

Many blast analysis tools are available to evaluate and predict the effects of blast 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 programs due to security reasons.

The level of detail presented and used in a blast analysis can vary by extremes. Corresponding to the level of detail is the cost—extremely detailed analyses can be very expensive, while simpler ones can be fairly inexpensive.

Engineers must 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 type of failure are obvious. Such an attack then 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 structure 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" (December 2003). Chapter 4 of this document discusses different methods by which designers can assess potential damage to their facilities

APPENDIX D

CHECKLISTS OF KEY POINTS FROM EACH SECTION

PART I - OVERVIEW CHECKLISTS

Section I-A - Introduction

None

Section I-B- Applicability Checklist:

☐ **Airports**
- New
- Existing
- Expanding
- Commercial Passenger
- General Aviation
- Major Cargo
- Multi-Modal

☐ **Users of this Book**
- Airport Operators
- Aircraft Operators
- Airport Tenants
- Planners
- Designers
- Architects
- Engineers
- Consultants

☐ **Projects**
- Planning
- Design
- Construction
- Renovation
- Assessment

☐ **Facilities**
- Terminals
- Cargo/Freight
- Police/Fire
- Maintenance
- Catering
- Roadways/Parking
- Tenant and Other On-Airport Facilities

Section I-C - Purpose Checklist:

☐ **Identify Key Concerns & Concepts in order to:**

- Restrict access to the AOA, SIDA & Secured areas
- Control the flow of people
- Provide efficient security screening
- Separate security areas
- Protect vulnerable areas & assets
- Protect aircraft, people & property
- Address blast mitigation measures
- Provide space for EDS & ETD devices
- Provide space for EOD operations

☐ **Identify Early Coordination needs with:**
- Airport Law Enforcement
- Emergency Response Agencies
- Fire Code Officials
- Building Code Officials
- Model Code Officials
- Operations and Maintenance Personnel
- Other End-Users

Section I-E - Coordination Checklist:

☐ **Initial coordination with the TSA FSD**
☐ **Get the early involvement of Airport Security Committee & others**
☐ **Assure 49 CFR and ASP requirements are met**
☐ **Consider the needs of law enforcement, emergency response, security and safety support personnel**
☐ **Reference *CBP Airport Technical Design Standards* at Airports where FIS areas are involved**

Section I-F - Security Concerns & Contingency Measures Checklist:

☐ **Discuss contingency needs with airport, TSA, FAA and aircraft operator officials**
☐ **Consider potential impact of contingency measures and emergency plans**
☐ **Consider potential impact on various areas (landside, airside, terminal, etc.)**
☐ **Consider the latest changes in security concerns**

Section II-A - General Checklist:

☐ **Advance Planning**
☐ **Continuous Monitoring**
☐ **Physical Security Program**
- Vulnerability assessment
- Periodic inspections
- Continuing security awareness/education
- Emergency procedures

- ☐ **Consult with Experts in Aviation**
- ☐ **Coordinate with Security/Regulatory Personnel**
- ☐ **Refer to Regulatory Requirements & Standards**
- ☐ **Coordinate with the TSA FSD**

Section II-B - Facility Protection Checklist:

- ☐ **Airport Security Committee Review**
- ☐ **Perimeter Protection - First Line of Defense**
- ☐ **Interior Controls - Second Line of Defense**
- ☐ **Cost Analysis**

Section II-C - 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
  - Wiring Requirements
  - Heavy-load Equipment
  - Effects on Passenger Flow
  - Construction Equipment Needs
  - Large-size Material Delivery
  - Seismic Requirements

Section III-A-1 - Airport Layout and Boundaries Checklist:

- ☐ **Analysis of General Security Requirements**
- ☐ **Security & Safety Considerations**
  - Separate dangerous or hazardous areas
  - Minimize concealed/overgrown areas
  - Effects on/by adjacent facilities
  - Natural features that might allow access
  - Prevent communications interference due to natural features, buildings & equipment
  - Public safety & security concerns
  - Criminal Activity
- ☐ **Airside**
  - Nonpublic
  - Maintain airside/landside boundaries
  - Maintain security clear areas and zones
  - Adequate emergency response routes
  - Required safety measures & 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 & safety
  - Public security & safety

Section III-A-2- Security Areas Checklist:

- ☐ **AOA**
  - Align AOA boundary with fences or natural boundaries
- ☐ **SIDA**
  - Part of AOA
  - Smallest manageable contiguous size(s)
- ☐ **Secured Area**
  - Consider general aviation, cargo, maintenance, and other facilities in a manner consistent with latest TSA regulation and policy guidance.
- ☐ **Sterile Area**
  - Minimize size to help surveillance and control
- ☐ **Exclusive Area**
  - Minimize areas to be monitored/controlled
- ☐ **ATSP Areas**
  - Minimize areas to be monitored/controlled

Section III-A-3 - 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 Way
- 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
- Delays
- Piggybacking
- Surveillance/CCTV

☐ **Plan for breach control measures and procedures**
- Physical Barriers
- Separation Distance

☐ **Reduce bombing/armed attack vulnerability**
- Blast Mitigation
- Separation Distance
- Minimization of 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**

Section III-A-4 - Chemical & Biological Agent Checklist:

☐ **Sources of guidance may include TSA, Federal Emergency Management Agency (FEMA), Federal Bureau of Investigation (FBI), Department of Energy (DOE), Center for Disease Control (CDC) and Office for Domestic Preparedness Support.**

☐ **The *Bibliography* lists several relevant chem-bio documents.**

Section III-A-5 - Boundaries & Access Points Checklist:

- ☐ **Boundary Choice Factors**
  - Equipment Cost
  - Installation Cost
  - Maintenance Cost
  - Effectiveness
  - Functionality
- ☐ **Physical Barriers**
  - Align with security area boundaries
  - Fencing
    - Select fencing type based on threat and vulnerability assessments, aesthetic considerations, and cost
    - Typically 7' chain link fabric + 1' barbed wire
    - Fence designs are available which are difficult to climb or cut
    - Select barrier types based on threat and vulnerability assessments, aesthetic considerations, and cost
      - Permanent barriers
      - Movable barriers
      - Bollards
      - Vehicle crash barriers
    - Motion, tension or other electronic sensing means available
    - Allow access points for vehicles and persons
    - In critical areas, anchor or bury the fence bottom
    - Keep lines straight and noncomplex
    - FAA References include:
      - Advisory Circular 150/5360-13
      - Advisory Circular 150/5370-10
      - 49 CFR 1542.201 & 1542.203
  - Buildings
    - May be used as a physical barrier
    - May be incorporated into a fence line
    - Assess security access points
  - Interior Walls
    - Security walls should be full height, floor-to-solid ceiling or to slab
  - Exterior Walls
    - Aesthetic designs available
    - Minimize hand & foot holds that can be used for climbing
    - Consider topping walls with barbed wire or other deterrent materials
- ☐ **Electronic Boundaries**
  - Electronic sensors
  - Motion detectors
  - Infrared sensors
  - Stand-alone or used with other barriers
- ☐ **Natural Barriers**
  - Bodies of water
  - Expanses of trees
  - Swampland
  - Dense foliage
  - Cliffs
  - Other areas difficult to traverse
  - Natural barriers may provide "time and distance" protection
- ☐ **Access Points**
  - Minimize the number of access points
  - Gates
    - Plan for routine, maintenance, and emergency operations:
      - Patrols
      - Emergency Response Teams
      - Service Vehicles and Tugs
      - Delivery Vehicles

- Maintenance Vehicles

- Design for high activity/long gate life
- Gate hinges should be non-liftoff or have welding to prevent removal
- Automate/Monitor gates as necessary
- Reduce ground clearance beneath, typically to no more than 4-6 inches
- Two-gate systems can help prevent “tailgate” entry (sally ports)
- FAA References include:
  - Advisory Circular 150/5300-13
  - Advisory Circular 150/5360-9
  - Advisory Circular 150/5360-13
  - Advisory Circular 150/5370-10

- Doors
  - Avoid unsupervised emergency exit doors to the AOA
  - Automate/Monitor doors as necessary
  - Coordinate hardware with building and fire codes
- Guard Stations
  - Manned access control and search capability
  - Size number of inspection lanes against predicted traffic volumes and inspection processing rates
  - Vehicle lane widths and heights should be matched to largest vehicle accessing the airport
  - Provide sheltered checkpoint station
  - Provide adequate secondary inspection space
  - Dependable communications required
- Electronic Access Points
  - Automatic Gates
    - Locate induction loop to minimize objects from the public-side activating loop
    - Consider bollards to reduce equipment damage by vehicles
    - Protect of electronic equipment from weather and temperature
  - Doors with Access Controls
    - Numerous technologies available
    - See RTCA DO-230A, “Standards for Airport Security Access Control Systems”
  - Sensor Line Gates
    - Function as access-controlled gates
    - Reduced delay time for access
    - Higher risk due to lack of barrier
  - Automated Portals
    - Designed for high-throughput
    - Can include screening technologies
    - Direction sensitive capabilities
    - Can detain violators
- Other Security Measures
  - Fencing Clear Zones
    - Both sides of fence
    - No obstructions
    - Minimal landscape
    - No climbable objects
  - Security Lighting
    - Both sides of gates and fencing is highly recommended
  - Locks
    - Various key technologies available
    - Consider total life cycle costs, not just initial capital cost
  - CCTV Coverage
    - CCTV can be used to enhance detection and/or response
  - Signage
    - Specific requirements are in ASP
    - TSA/FAA-required signage per Advisory Circular 150/5360-12C
    - Deterrent signage

- Instructional and/or legal signage
- Coordinate with airport signage policy

Section III-A-6 - Facilities, Areas and Geographical Placement Checklist:

☐ **Facility Placement Considerations:**
- Interaction and relationships among areas
- Types of activity within each area
- Flow of public/employees to/through areas
- Flow and type of delivery traffic
- Flow and type of maintenance traffic
- Need for and frequency of security escorts
- How each area is addressed in the ASP

☐ **Each Airport is Unique**

☐ **Facilities:**
- Aircraft Maintenance Facilities
  - Airside, Landside or Both
  - Security the responsibility of the facility
- Aircraft Movement Areas
  - Airside
  - Requires controlled access
- Passenger Aircraft Overnight Parking Area
  - Airside
  - Requires controlled access
- ARFF Facilities
  - Either Airside or Both
  - Consider response routes and times
  - Facility may require public access
- SOC/CP
  - Secure location
  - Consider alternate/back-up locations
  - Ease of airside access
  - Sufficient operating space for personnel
  - Central location for dispatching
  - See Terminal Nonpublic Areas Checklist
- Airport Personnel Offices
  - Airside, Landside or Both
  - Consider security needs
  - See Terminal Nonpublic Areas Checklist
- Belly Cargo Facility
  - Airside, Landside or Both
  - Flexible Placement
  - Terminal Access (via roads) required
  - Consider cargo screening needs
- Cargo Area
  - Typically Airside or Both
  - Screening and inspection needs
  - Secure cargo-holding area
  - Postal facility inclusion possible
  - Doors must be lockable and controlled
  - Consider fence protection measures

- FAA ATCT and Offices
  - Landside or Airside
  - May require airport security controls
- Fuel Area
  - Landside or Airside
  - Typically remote from terminal
  - Safety and security fencing required
  - Consider access controls to area
- GA Areas
  - Typically Airside on Both
  - Boundaries based on function
- GSEM Facility
  - Landside or Airside
  - Consider airside travel frequency
  - Maintain fencing clear zones
- GTSA
  - Landside
  - Public Safety and Security Concerns
- Hotels and On-Airport Accommodations
  - Landside
  - Public Safety and Security Concerns
- Industrial/Technology Parks
  - Landside, Airside or Both
- In-Flight Catering Facility
  - Landside, Airside or Both
  - Typically adjacent to terminal
- Intermodal Transportation Area
  - Typically Landside
- Military Facilities
  - Substantial coordination required
- Navigation and Communications Equipment
  - Airside and Landside
  - Driven by functionality
  - Control access to critical equipment
- Rental Car Facilities
  - Landside
  - Public Safety and Security Concerns
- State/Government Aircraft Facilities
  - Both airside and landside
  - Security typically independent
  - Coordinate security requirements
- Utilities and Related Equipment
  - Locate airside when possible
  - Control access
  - Secure access points and equipment

Section III-B - Airside Checklist:

☐ **Aircraft operations areas must be secured**

☐ **Factors influencing boundary locations:**

- Aircraft Movement Areas

        - Runways, taxiways, ramps and/or aprons (See A/C 150/5300-13)
        - FAA safety and operational areas (See CFR Part 77)
            - Object Free Area
            - Building Restriction Lines
            - Runway Protection Zone
            - Runway Safety Area
            - Glide Slope Critical Area
            - Localizer Critical Area
            - Approach Lighting System
    - Passenger Aircraft Parking Areas
        - Safe distance to fence/public access areas
        - Safe distance to other parked aircraft
        - Safe distance recommendations for prevention of vandalism
        - Maintain visibility of areas around parked aircraft to monitor for unauthorized activity
    - General Aviation (GA) Parking Area
        - Exclude GA from the SIDA
        - Distance GA from terminal area
        - Coordinate with tenants
    - Isolated/Security Parking Position (See ICAO Standards Annex 14 & 17)
        - At least 100 meters from other aircraft and structures
        - Ensure separation from utilities and fuel
        - Use CCTV to view the aircraft and surrounding area
        - Accommodate emergency staging area
        - Avoid public viewing/proximity to area

☐ **Airside Roads**
- Restrict access to authorized vehicles
- Perimeter roads should be airside
- Perimeter roads should provide unobstructed 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 ATCT

Section III-C - 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 AOA/security fencing
- Pre-terminal screening capability
- CCTV monitoring for security/safety

☐ **Landside Parking**
- Terminal Passenger Parking
  - Allow significant distance between parking lots and terminals
  - Consider CCTV, lighting, intercoms, and duress alarms for toll plazas
  - 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 and safety concerns include:
    - Driver safety
    - Deterrence of vandalism, theft or other illegal activity
    - Possibility of terrorist or criminal assault
  - Planning/design measures may include:
    - Limitation of concealed areas and locations
    - Provisions for open stairwells
    - CCTV surveillance of the area
    - Duress alarms in restroom and/or public areas
    - Structural layout that minimizes or distributes congested driver waiting areas
    - Sufficient night lighting
- Hotels and On-Airport Accommodations
  - Possibly connected to terminal
  - Treated no differently than other commercial areas
  - Limit direct line of sight of aircraft
  - Maximize distance to AOA
- Intermodal Transportation Area
  - Mass transit and light rail systems may require secured transitions
  - Provide adequate standoff distance between transit station and the AOA
- Rental Car Storage Areas
  - Protect vehicles and workers
  - Potential tie-in to airport access controls
  - Maintain AOA fencing clear zones

☐ **Off-Airport Emergency Response**
- Consider access routes, methods and needs
- Design features may include:
  - Special identification media, PIN numbers or card readers for emergency access
  - Emergency Access to terminal areas

Section III-D-1 - Terminal Security Architecture Checklist:

- ☐ **Architecture plays a fundamental role in transitioning from public to secured areas**
- ☐ **Design to be flexible; technology, regulations, and threat continues to change**
- ☐ **Carefully coordinate locations for access points and equipment rooms to minimize crossing security boundaries during day-to-day operations**
- ☐ **Planning and Design Considerations**
  - Physical Boundaries
  - Between different regulatory and physical security levels
  - Prevent items from being passed through/over
  - Deter public access to nonpublic areas
  - Provide visual or psychological deterrent
- ☐ **Bomb/Blast Analysis**
  - Critical part of early design considerations
  - Review bomb/blast analysis periodically
- ☐ **Limited Concealment Areas/Structures**
  - Minimize areas where objects or persons can be concealed
  - Minimize and lock accessible spaces and rooms
  - Coordinate with local security, search and threat response agencies
- ☐ **Operational Pathways for:**
  - Passengers
  - Airport Personnel
  - Tenants / Concessions
  - Emergency Response Routes
  - Delivery Routes
  - Security Response
  - Police Escorts for Holding Purposes
- ☐ **Minimum Number of Security Portals**
  - Minimize numbers for cost and security
  - Reduces cost if personnel screening becomes necessary
  - Maximizes use/efficiency of systems
  - Remain flexible for future expansion
- ☐ **Space for Additional Security Measures**
  - Allows growth with minimal impact on operations
  - Reduces installation and execution costs
  - Reduces time needed for additions/expansions
- ☐ **Consider allotting space/accommodations for:**
  - Temporary SSCP
  - Additional SSCP locations
  - Delivery and personnel screening
  - Expansion to planned SSCP (Refer to the *SSCP Section* on page 88 for further information)

Section III-D-2 - Terminal Area Users and Infrastructure Checklist:

- ☐ **Meet with all relevant airport users and stakeholders, including tenants and government agencies.**

☐ **Personnel circulation includes vertical separation as well as horizontal (elevators, escalators, stairwells)**

☐ **Supporting utility infrastructure (power, data, communications) is an equally important element of security design**

☐ **New Construction vs. Alterations – both require the same attention to security**

Section III-D-3 - Sterile Areas Checklist:

☐ **Sterile Areas**
- Refers to the area between the security screening checkpoint and the aircraft loading bridge and/or hold room door.
- Primary objective; passenger containment, preventing access to weapons or contraband
- Number of access limited to the minimum operational necessity
- Comply with local fire and life safety codes, Americans with Disabilities Act (ADA), etc.
  - Prevent articles from being passed from non-sterile areas to sterile or secured areas
  - Consider pathways in restrooms, airline lounges, kitchen facilities, plumbing chases, air vents, drains, trash chutes, utility tunnels or other channels
  - Consider access needs of airport and airline personnel, maintenance and concession staff and supplies
- Tenant personnel and airport employees who require access into the sterile area from public occupancy areas
- Emergency response routes and pathways
- Routes for off-airport response, emergency medical services [EMS] and fire personnel
- Concessionaires have unique access, delivery and storage requirements beyond security, including perishables
- Built-in security-friendly fixtures (i.e., railings, pillars, benches, ashtrays, trash cans, etc.) are widely available

---

Section III-D-4 - Public Areas Checklist:

☐ **Public Areas**
- Public Lobby Areas (Ticketing, Bag Claim, Rental Car)
  - Limit the number of access points
  - Monitor all access points and conveyor belts via CCTV
  - Visually differentiate public and secure or restricted areas
  - Build in a capability to secure areas when not in use
  - Select furnishings and accessories which avoid the concealment of explosives
  - Seek advice from structural and explosives experts on minimizing the effects of blast
  - Ticketing Lobby
    - Minimal seating in ticketing lobbies will reduce congestion
    - Consider the needs of international or high-risk aircraft operators with extended security measures during the passenger check-in process
    - Additional queuing space may be required
- Public Emergency Exits
  - Some exit requirements have specific widths and separation distances
  - Coordinate locations closely with the Fire Marshall and/or Code officials

- Emergency exits should avoid moving persons from areas of lower security to areas of higher security
- The number of emergency exits leading into secured areas should be minimized
- Exiting screened individuals should be kept separate from unscreened individuals
- Consider emergency doors with push-type panic bars with 15-30 second delays (where allowable)
- Security Doors vs. Fire Doors
  - If the door is not a fire door, make it lockable
  - Emergency egress door (fire door) may not be locked

- Concessions Areas
  - Consider a design to accommodate moving concessions (or screening points) during heightened security
  - Some concessions require storage and processing space
  - Look for short delivery and personnel access routes that minimize crossing security boundaries
  - Consider type of concession, delivery, storage, moneyhandling and security escorts, ATM security
  - Design elements for concessions include:
    - Locate concessions storage areas in public or nonsecured /low-risk areas
    - Separate loading dock/concessions screening area from passengers and secured areas
- Vertical Access: Prevent public access to the airside though connecting elevators, escalators and stairwells
- Signage: Types of agencies with interests in signage at airports:
  - Accessibility
    - Americans with Disabilities Act (ADA)
    - Americans with Disabilities Act Accessibilities Guidelines (ADAAG)
    - Disability and Senior Citizen Groups
    - State Accessibility Codes
  - Government Agencies
    - Federal Aviation Administration (FAA)
    - Department of Transportation (DOT)
    - Department of Justice (DOJ)
    - Occupational Safety & Health Administration (OSHA) Port Authority
  - Federal Inspection
    - Customs and Border Protection (CBP)
    - CBP Airport Technical Standards 2004
    - Animal and Plant Health Inspection Service (APHIS)
    - Fish and Wildlife Service (FWS)
    - Center for Disease Control (CDC)
    - Public Health Service (PHS)
  - Building Code Compliance
    - Local building and fire codes
    - State building and fire codes
    - Electrical Code
    - Life Safety
  - Security
    - Airport Police
    - Transportation Security Administration (TSA)
    - Department of Homeland Security (DHS)
    - Foreign Language Specialists (Translation Services)
    - Media Relations/Public Relations
  - Signage specific coordination required:
    - Electrical (providing power and data to signs)
    - Video/Cameras (obstructions)

- Sprinkler Systems (obstructions)
- Lighting (obstructions and/or external illumination of signs)

- Lockers:
  - Eliminate public lockers from public areas where possible
- Unclaimed luggage areas – landside, with easy EOD / LEO access
- VIP Lounges/Hospitality Suites
  - Consider location in relationship to sterile area
  - Prevent unauthorized access to secured and sterile areas
  - Provide space for monitored baggage holding facilities
- Observations decks are strongly discouraged - Where they exist, they should be closed to public access

Section III-D-5 - Nonpublic Areas Checklist:

☐ **Non-Public Areas**

- Service Corridors, Stairwells and Vertical Circulation
  - Service corridors should not cross boundaries of secure areas
  - Service corridors may be used to minimize quantity of security access points
  - Tenant areas can be grouped into common service corridor
  - Consider corridor placement and use by airport emergency personnel and law enforcement
  - Fire stairs typically connect many of the building's floors/levels as well as security areas
  - Stairwells and vertical pathways may require security treatments and boundaries
- Airport Personnel Offices
  - Office areas should connect via corridors and stairs to minimize the need to cross security boundaries
  - Office spaces should be planned to accommodate visitors and public access
  - Consider the use of satellite police, ID or first aid offices
- Tenant Spaces
  - Some tenant spaces might require tie-in to the airport access control and alarm system
  - Consider tenant money-handling, overnight operations, early morning concession deliveries
- Law Enforcement & Public Safety Areas
  - Public Safety or Police Offices
    - Office space for airport law enforcement in the terminal
    - Public access area protected with ballistic materials, laminates, concrete bollards, etc.
    - Include adequate space (in no particular order) for:
      - Briefing/work room
      - Training classroom/offices
      - Property/evidence room(s)
      - Conference rooms—can be part of CP/operations room(s)
      - Holding cells
      - Possible satellite locations
      - Private Interrogation/Witness Statement room(s)/area
      - Physical fitness area in conjunction with lockers, showers, and restrooms
      - General storage areas
      - Secured arms storage
      - Kitchen/lunchroom facilities
    - Areas requiring access for public and tenants but protected with adequate controls are:
      - Administrative offices
      - Security ID offices
      - Lost and found
      - SIDA/tenant training rooms

        - Medical services
      - Consider electrical, fiber optic and other utility supply and routes to/from the police areas
    - Law Enforcement Parking
      - Accessible, with direct landside/SIDA access
    - Remote Law Enforcement/Public Safety Posts/Areas
      - Consider remote law enforcement posts or substations; outdoor shelters
    - Other Considerations
      - Communication/Dispatch facilities
      - Equipment repair areas
- Dogs/K-9 Teams
  - If there is no on-site K-9, specify non-critical area for temporary K-9 use
  - Rule of thumb: a 4- by - 8-foot indoor pen, 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, dry environment, without mildew or dampness
  - The dog area should be secured, and sufficiently isolated from casual public contact
  - Provide areas for veterinarian services and training activities
  - Isolation from noise and odor sources, especially jet fuel fumes
  - Secured storage for explosives test and training items; coordinated with ATF
  - Consider proximity to EOD personnel and to threat containment units
- Security Operations Center (SOC)
  - Consider multiple communications options for police, fire, rescue, airport operations, crash/hijack alert, off-airport emergency assistance, and security of communications
  - Locate close to the Airport Emergency Command Post (CP), in a secure area
  - For cabling interconnections, a central geographic location maintains reasonable cable lengths
  - Floor space, cabinets, power, HVAC, fiber optics and cabling, and conduit paths
  - Rear access to console for maintenance and update.
  - Consider space requirements of consolidating all functions within the SOC:
    - Airport Police and/or Security Department
    - Automatic Notification System for emergency response recall of personnel
    - Direct phone lines to ATC tower, airlines, airport mini hospital, etc.
    - Fire Alarm monitoring
    - Flight Information Display (FIDS) systems; Baggage Information (BIDS) systems
    - ID offices
    - Information Specialists for customer information phones, paging;
    - Landside/Terminal Operations
    - Maintenance Control/Dispatch (includes total energy management of HVAC systems)
    - Airport Radio and Personnel Paging Systems
    - Recording Equipment
  - Plan an alternate site capable of supporting the basic operation.
  - A direct view of the airside and the isolated parking position is desirable.
  - Space Needs
    - Space for Crisis Management Team's Operational Group and Negotiators
    - Advisory Circular 150/5200-31A on airport emergency planning can assist
  - Other Considerations
    - Raised flooring is an option for installation of ducts and cable paths.
    - CP electrical power must be uninterrupted
    - Vehicular access to the CP necessary
    - Controlled parking for support vehicles and key CP vehicles
    - Provide space for kitchenette and rest rooms.
- Family Assistance Center – designated space in the case of an accident or incident.
  - FIS areas are designed toward very different law enforcement and security situations

  - FIS agencies publish a separate document that provides their additional security design guidelines required within their operational spaces
  - Reference FAA Advisory Circular AC 150/5360-13
- Loading Dock & Delivery Areas
  - Access control and identification media
  - Package screening
  - CCTV
- FIS Areas

SEE: FAA Advisory Circular 150/5360-13, Planning and Design Guidelines for Airport Terminal Facilities.

http://www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgAdvisoryCircular.nsf/0/3E90EF87705845186256C69007504BE?OpenDocument&Highlight=150/5360-13

Section III-D-6 - Terminal Vulnerable Areas and Protection Checklist:

☐ **Due to the complex/multi-use function of terminals they contain the broadest range of vulnerable areas**

☐ **Each airport is unique and must 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 adjacent 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 and switching gear
- 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

Section III-D-7 - Chemical & Biological Agent Checklist:

☐ **Sources of guidance may include TSA, Federal Emergency Management Agency (FEMA), Federal Bureau of Investigation (FBI), Department of Energy (DOE), Center for Disease Control (CDC), and Office for Domestic Preparedness Support.**

☐ **Consider position of vent intakes; HVAC system capacity for airflow management**

☐ **Consider areas for quarantine, detox, chem-bio screening of people and vehicles; capacity to accommodate outside mutual medical aid.**

☐ ***See also*, Edwards, Dr. Donna M., *et al,* "Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism," Sandia Report SAND2005-3237, Berkeley Lab Report LBNL-54973 (May 2005), Prepared by Sandia National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550.**

Section III-E-1 - Security Screening Checkpoints (SSCP) Checklist:

☐ **Passenger SSCP issues**
- General issues
- Regulations & Guidelines – 49 CFRs 1542, 1544, 1546
- Essentials
- TSA, Airport and airline personnel should be consulted
- Planning Considerations
  - Level and type of risk
  - Airport operational type
  - Location of SSCP
- Elements of the SSCP
  - **A** - Prescreening preparation instruction zone
  - **B** - Queuing Space
  - **C** - Walk through metal detector (WTMD)
  - **D** - Non-metallic barriers
  - **E** - Non-metallic ADA Gate/Access
  - **F** - Carry-on baggage X-ray machine
  - **G** - Divest & Composure Tables
  - **H** - SSCP adjacent walls / barriers
  - **I** - Holding Stations
  - **J** - Wanding Stations
  - **K** - ETD machines
  - **L** - Egress Seating Area
  - ETP
  - Supplemental X-Ray
  - LEO Station
  - Supervisor Station
  - Private Search Area
  - CCTV Coverage
  - Data Connections/Cabinet
  - SSCP Lighting
  - Wireless Access Point
  - Exit Travel Lane
  - Exit Lane Station
  - Exit Lane CCTV
  - Integrated Exit Lane Systems
- SSCP Operational Efficiency
  - Designing for the Process
  - Length of Response Corridor
  - Architectural Design to Support Intuitive Processes
  - SSCP Signage
  - Space for TSA Staff
- SSCP Layout Standards
- SSCP Spacing Requirements
- SSCP Project Funding
- Designing for the Future
  - Bulk Explosives Detectors
  - Multi-detection tunnel
  - Remote Screening/monitoring room

Section III-E-2 - Baggage Screening Checklist:

- ☐ **Applicable Regulations**
  - Regulatory Requirement
  - TSA Protocols
- ☐ **Protocols and Concept of Operations**
  - Checked Baggage Screening Options
    - Category 1: Fully Integrated In-Line Systems
    - Category 2: In-Line Systems
    - Category 3: In-Line or Ticket Counter Mounted Systems
    - Category 4: Stand-Alone EDS
    - Category 5: Stand-Alone ETD Systems
    - Category 6: Emerging System Technology
  - ETD and EDS Key Performance Characteristics
  - Design Goals
    - Schedule Issues
    - Fail safe Screening
    - Maximizing Automation
    - Baggage Handling
      - Minimizing Baggage Delivery Time from Check-In to Make-Up
      - Diversion of Out-of-Gauge Bags
      - Oversized Bags
      - Diversion of Alarmed Bags
      - Handling of Selectee Bags
      - International Connecting Bags
    - Capacity Concepts
    - System Maintainability
    - Ergonomics
    - OSRF
    - CBRA
    - Suspect Bag Removal
    - Contingency Plans
    - Environmental Impact
    - Communications
    - Engineering Issues
      - Maintenance Access and Removal
      - Floor Loading
      - Systems Integration and Operation
    - ADA
    - CCTV
      - Surveillance
      - Operational
- ☐ **Design Mitigation**
  - Lessons Learned
    - Avoid Steep Conveyor Slopes
    - Manage Belt Speed Transitions to Avoid Tracking Loss
    - Photo Eyes Too Close to the Belt
    - Avoid Placing Photo Eyes Too Close to Conveyor Ends
    - Avoid Static-Plough and Roller Diverters
    - Use Conveyor Brakes and VFD
    - Avoid Inaccurate Pusher Operation
    - Avoid Improper Merging and Too Many Merges
    - Avoid 90 Degree Merges
    - Avoid In-Line Decision and Removal Points

- Avoid Directly Opposing Diverters
- Lack of Decision Point Fail-Safe
- Avoid Re-Insertion Points Between EDS and Decision Point(s)
- Avoid Bottlenecks
- Avoid Using Plexiglas Photo Eye Guards
- Avoid Short Reconciliation Lines
- Avoid Non-Powered Rollers
- Avoid Power Turns at the EDS Exit
- Use Tubs When Appropriate
- Consider How Bag Orientation to EDS Will be Maintained
- Use Caution with Draft Curtains
- Avoid Tracking without Real-Time Belt Speeds
- Inefficient Baggage System
- Efficient Baggage System

☐ **Impact of Various Threat Levels on Screening Operations**
- Temporary space for baggage staging
- CBRA search area(s)
- Suspect bag retention and removal area
- Reasonable vehicle access (e.g., Tug, pick-up, police vehicle)

☐ **Alternative Screening Options (Remote Screening)**
- Remote Baggage Check-In

☐ **Evaluating Design Options**
- Define Performance Goals
- Determine the Appropriate Planning Horizon
- Evaluating the Performance of the Proposed Solution

Section III-E-3 - Cargo Screening Checklist:

☐ **Access points addressed**
☐ **Access points for employees/ contractors**
☐ **Space for additional technology, staffing requirements**
☐ **Sorting areas, separate from acceptance areas**
☐ **Separation and security of cargo prior to and post inspection**
☐ **Accessibility of building to commercial entities/ employees**
☐ **Perimeter needs**
☐ **Facilities for employees**
☐ **Postal facility inclusion**
☐ **Emergency response factors**
☐ **Inclusion of specialized personnel in determining security concerns**

Section III-F - ACAMS Checklist:

☐ **Power Requirements**
- Emergency power systems/battery back-up for servers
- Emergency power systems/battery backup for control panels
- Emergency power systems/battery backup for operating stations
- Emergency power systems/battery backup for door hardware

☐ **Data and Communications requirements**
- Sever to panel communications
- Panel to door communications
- Server to dispatch area requirements
- Wherever possible a security network should run on physically separate dedicated and protected systems from non-security systems.

☐ **Security System Infrastructure**
- Separation from non security infrastructure
- Controlled access
- Access for maintenance
- Secure access for management

☐ **Potential Equipment Placement Locations**
- Terminal Area Access Points
  - Secure area access Personnel Doors
  - AOA access Personnel Doors
  - Sterile Area Access Personnel Doors
  - Concourse area entrances (grills)
  - Inbound/Outbound Baggage Doors
  - Inbound/outbound Baggage Doors control
  - Loading Dock Doors to Secure/Sterile/SIDA/AOA
  - Service Corridor and Stairwell Doors
  - Administrative Office Doors
  - Telecom Room Doors
  - Maintenance Area/Equipment Room Doors
  - Tenant and Concessions Area Doors
  - Roof Access Points
  - Manhole access points
  - Fire/Emergency Exit Doors
  - Material Storage/Safe Areas
  - Display/Museum/Art Cases
  - Hazardous material storage areas
  - CBP areas
  - TSA offices
  - EDS operation areas
- Terminal Duress/Convenience Alarms
  - Passenger Screening Checkpoints
  - Baggage Screening Areas
  - Ticketing/Rental Car Counters
  - Administrative/Information Desks
  - Companion Care/Family Restrooms
  - Police Substations/First Aid Areas
  - Chapels
  - Concession/Retail Cash Registers
  - Dispatch and communication locations
- Site Access Points
  - AOA/SIDA/Secure Vehicle Gates
  - Maintenance/Personnel Gates
  - Non-Terminal AOA/SIDA Doors
  - Site Telecom Room Doors
  - Maintenance Building Doors
  - Tenant Facility Doors
  - Navaids and FAA facilities
  - Cargo Facilities
  - Perimeter gates

- Site Alarm Points
  - Material Storage Areas
  - Parking Management/Tenant Safes
  - Critical Equipment Locations
- Site Duress/Convenience Alarms
  - Parking Toll Booths
  - Parking Management Office Money-Handling/Storage Areas
  - Public Parking and Garage Areas
  - Ground Transportation/Taxicab Booth Areas
  - Administrative/Reception Areas
  - Tenant/Cargo Cash Register Areas
  - Airport/Tenant Guard Booths

☐ **Dispatch requirements**
- Monitoring locations should be in a secure area
- Monitoring location should be separate from normal offices
- Monitoring locations should be part of an integrated incident dispatch program
- Monitoring locations should have relevant CCTV access capability
- Alternate monitoring capability location should be provided.
- Monitoring location should be separate from admin and identification (ID) locations

---

Section III-G Surveillance and Video Detection Systems Checklist:

☐ **Establish Operational Requirements**
- Review surveillance needed at each site
- Camera Placement and Mounting
  - Security
  - Access for Maintenance
  - Appearance and Aesthetic Issues
- Field coverage
  - Fixed
  - Variable (pan/tilt mounts)
- Camera Resolution and Lens Focal Length (magnification) required for
  - Detection
  - Classification
  - Identification
  - Recognition, including law enforcement requirements
- Intelligent Video Functions – to enhance video performance and reduce personnel
  - Target Tracking
  - Discarded/Abandoned Object Detection
  - Software-based rather than dedicated appliances
- Special Coverage of Security Checkpoints
- Lighting
  - Exterior Perimeter
  - Interior Areas
  - Infrared (non-visible) Lighting
- Video Storage
  - Duration
  - Resolution
  - Frame Rate

☐ **System Design and Equipment Selection**
- Balance operational requirements, functionality, cost, and security

- Information Retrieval and Distribution
  - Privacy
  - Statutory Constraints
- Reduce security force and police response requirements
- Power/Data – power outlets for each video camera
  - Power from emergency operating conditions
  - Battery backup not required
- Camera Selection and Interfaces
  - Type – analog or IP, color or monochrome – or a mix
  - High-light (bright spot) and low-light lever performance
  - Infrared (thermal) Imagers – for special areas
  - Link CCTV to ACAMS alarm signals
  - Pan/tilt/zoom camera mounts – used to minimize camera quantities, provide redundant coverage, reduce personnel required for monitoring
  - Mount cameras in locations with accessible ceilings/cabling route
- Video Storage
  - Architecture and Storage Strategy
  - Hard Drive Capacity
  - Local and network storage
  - Scalability
  - Management
  - Emergency Backup
- Networked Video Cameras
  - Network Architecture – design to minimize bandwidth required
  - Browser User Interface
  - Storage Network Interfacing
  - Network Security
- Displays and Security Operations Center
  - Ergonomics – design for extended and emergency operations
  - Integrated video feeds to minimize display quantities
- Remote (off-site) Video Access
  - Browser User Interface
  - Secure Access
- Camera Installations – derived from operational analysis of surveillance required
  - Ticket Counters
  - Kiosks
  - Terminal Apron
  - Security Checkpoint Areas
  - Public Lobby Areas
  - Roadway/Curbside Baggage Areas
  - Loading Dock/Police Parking Areas
  - Administrative and Tenant Areas
  - Airside Access Doors and Gates
  - Baggage Handling and Claim Areas
  - FIS Areas
  - ACAMS Access Points
  - Runways and Taxiways and Airfield
  - Cargo/GA/FBO Ramps
- Public and Employee Parking Areas

☐ **Procedures and Personnel**

- User-Friendly Design
- Maximum 4 Monitors per Operator
- Training Plan
- Emergency Operations Plan
- Emergency Maintenance Plan

- Planned Maintenance/Outage Plan
- Equipment Service Tracking
- Periodic Upgrade/Evaluation

Section III-H - Power, Communications & Cabling Infrastructure Systems Checklist:

☐ **Secure components of the power, communications and infrastructure systems for reliable emergency operation**

☐ **Power**
- 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
- High amperage/ high voltage systems for such things as x-rays and explosives detection equipment
- Location and capacity of stand-by generators
- Installation of redundant power lines to existing and alternate locations
- Strong consideration to the installation of power lines, or conduit and pull-strings, to known future construction such as expanded terminal concourses

☐ **Cabling Infrastructure Systems & Management**
- Cabling Management
  - Determine standards for type and location of cabling and related infrastructure
  - Determine labeling, color-coding or other identification methods
  - Determine whether to identify security cabling/infrastructure

☐ **Security of Airport Networks**
- Network Availability Considerations
  - Dual (or multi-) network cabling to interconnect mission-critical equipment and platforms
  - The dual network cables may be laid along different paths to minimize the chances of damage
  - Redundant repeaters, switches, routers and power supplies, shall be considered
  - Separate wiring closets may host the redundant equipment
- Network Security
  - Protect networks from unauthorized access by external connections
  - Encryption has important design aspects for securing a general network
  - Shared vs. dedicated fiber is a design/cost issue to be examined with the IT designer
- Network Accessibility
  - WAN connectivity may be a consideration for Internet and/or Virtual Private Network (VPN) access
  - Airport may provide shared networking
- Information Storage Availability
  - Storage systems for mission-critical file server and database should be highly reliable
  - Take into account storage redundancy and back up
  - Pre-allocation of separate facility rooms for redundant storage system equipment
  - Put distance between storage rooms to reduce chances of all rooms being damaged

☐ **Future Rough-Ins/Preparations**
- Comprehensive early planning can significantly reduce future construction costs

- For future terminal expansion, additional concourses and/or gates, new buildings, or expanded or relocated security screening points with known locations, include extra conduit, pull strings, cable or fiber, terminations, shielding and other rough-in elements

☐ **Telecom Rooms**
- Design telecomm rooms, termination closets, wire rooms, in short direct line to each other
- Provide sufficient working space; accommodate known expansion requirements, including 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
- This area will also have additional cooling, fire protection, and dust control requirements

☐ **Radio Frequency (RF)**
- Three broad considerations in using RF-based communications
  - Efficiency and cost
  - Potential interference with other operational elements, including aircraft and air traffic communications, security operations, or general administrative data transfers

☐ **Physical Environment Concerns**
- Weather considerations
- Temperature
- Rain
- Snow
- Dust and dirt

☐ **Regulations - Coordinate with FCC, FAA, and TSA**

☐ **Installation Considerations**
- Antenna location, mounting, and directional/omni-directional considerations
- Other transmitters that have the potential to “interact” with airport systems
- Obstructions
- Coverage areas (and dead spots)
- Robustness of link
- Mobile or Portable
- Shielding
- Effect, if any, on ATC communications

☐ **Communications**
- Access to Main communication bus
- Network Access Security

☐ **Other Considerations**
- Interference is two-way
  - Higher frequency systems have more directional antennas, so emission can be better controlled.
  - “Outside the building” RF environment is unpredictable, requiring internal 'isolation'.
- Choke Effects Integral to Construction
  - At the low frequencies, wavelengths are long and can 'match' terminal openings
  - Subsurface metal rods, I-beams, etc. that ‘surround’ these openings, can create an effective RF choke
  - Adjusting passageway opening size can 'better tune' the choke
- Other Lessons Learned
  - Electrical and electronic environment at commercial airports rarely remains constant
  - There is always more that can be done to improve the EMC status
  - Loading bridge orientation can reduce unwanted radiation

Section III-I - International Aviation Security Checklist:

☐ **Establish Security Plan for FIS**

- Contact CBP and other Federal Agencies
  - Obtain CBP Airport Technical Design Standards
  - Obtain Workforce Analysis Model (WAM).
- Address CBP Issues in FIS Security Plan
  - Protection Strategy
  - Physical Safeguards
  - Plans and Procedures for Implementation/Management
  - Resources Required to Sustain FIS Protection Program
  - Evacuation Routes, Assembly Areas, Staffing
- Coordinate FIS Security Plans and Requirements with Airport Security Plan (ASP)
  - Access Control
  - CCTV
  - Baggage Screening and Explosives Detection
  - Perimeter Protection, including blast protection
  - Video, Voice, and Data Networking

☐ **FIS Design, Construction, Acceptance and Occupancy**

- Provide for CBP/Agency Involvement in Design and Construction Process
- Design Specifications, Drawings, and Construction Documents
  - Schematic Design
    - Model variability in processing times and passenger flow through exit control using the CBP Workforce Analysis Model (WAM) to size FIS
    - Architectural Integration
    - Security Integration
    - IT Integration
  - Design Development
  - Construction Bid Package
  - Obtain written approval(s) from CBP/Agencies at each step in this process
- Establish Change Review/Approval Process with CBP
- FIS Inspection and Acceptance
- FIS Occupancy

APPENDIX E

GLOSSARY*

**For the purposes of this document – definitions and terms defined by regulations, international standards or standard operating procedures have been noted. They are for the purpose of clarity as they are used in this document, and are subject to change. Other definitions may apply in other contexts.*

40/40/20[9]	An explosives trace detection screening protocol in which a percentage of checked baggage is screened using closed bag search (40%), limited open bag search (40%), and full open bag search (20%) procedures
50/50[9]	An explosives trace detection screening protocol in which the maximum amount of checked baggage possible, not less than 20% of all baggage, to include all selectee checked baggage, is screened with EDS and the remaining checked baggage is screened using closed bag search (50%) and limited open bag search (50%) procedures
9/11	September 11, 2001
A/C	Advisory Circular
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.
Adaptive Intelligent Screening	This method of EDS baggage screening involves active communication between the levels of screening and bag handling system so that, in addition to selectee bags, other bags are routed to EDS equipment or screened at the highest-level detection equipment on a bag-by-bag basis.
ADA	Americans with Disabilities Act
Administrator[1]	The Under Secretary of Transportation for Security identified in 49 U.S.C. 114(b) who serves as the Administrator of the Transportation Security Administration.
ADPM	Average Day Peak Month
AEP	Airport Emergency Plan
AES	Advanced Encryption Standard
AHU[10]	Air-Handling Unit
AIP[4]	Airport Improvement Program (AIP) by the Federal Aviation Administration (FAA). The Act'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. The Act provides funding for airport planning and development projects at airports included in the National Plan of Integrated Airport Systems (NPIAS).

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

Air Carrier[1]	A person or company undertaking directly by lease, or other arrangement to engage in air transportation. Also known as Aircraft Operator.
Air Carrier[3]	A person who undertakes directly by lease, or other arrangement, to engage in air transportation. This includes an individual, firm, partnership, corporation, company, association, joint-stock association, governmental entity, and a trustee, receiver, assignee, or similar representative of such entities.
Air Carrier Aircraft[3]	An aircraft that is being operated by an air carrier and is categorized, as determined by the aircraft type certificate issued by a competent civil aviation authority, as either a— large air carrier aircraft if designed for at least 31 passenger seats or small air carrier aircraft if designed for more than 9 passenger seats but less than 31 passenger seats.
Air Carrier Operation[3]	The takeoff or landing of an air carrier aircraft and includes the period of time from 15 minutes before until 15 minutes after the takeoff or landing
Aircraft Loading Bridge	An aboveground device through which passengers move between an airport terminal and an aircraft. (Often referred to by the brand name Jetway)
Aircraft Operator[1]	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. In specific parts or sections of 49 CFR, "aircraft operator" is used to refer to specific types of operators as described in those parts or sections.
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.
Air Operations Area[1]	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.
Airport[3]	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 Emergency Command Post	An airport emergency command post is 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.
Airport Operating Certificate[3]	A certificate, issued under this part, for operation of a Class I, II, III, or IV airport.

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

Airport Operator[1]	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 make decisions or issue directives.
Airport Security Program[1]	A security program approved by TSA under 49 CFR 1542.101.
Airport Tenant[1]	Any person, other than an aircraft operator or foreign air carrier that has 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[1]	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 §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 which service and maintain aircraft.
Airside[2]	The movement area of an airport, adjacent terrain and buildings or portions thereof, access to which is controlled.
Alarm[9]	An audible sound emitted from an ETD device. This SOP also uses the term when the EDS alerts the operator to a possible or obvious threat
Alarm Resolution[9]	To resolve an alarm during any part of the checked baggage screening process and determine whether an individual's property possesses prohibited items
ANSI	American National Standards Institute
AOA	**Air Operations Area**
AOSSP	Aircraft Operator Standards Security Program (AOSSP or SSP), the detailed, nonpublic document an aircraft operator regulated under 49 CFR 1544, must implement in order to meet TSA's minimum security standards. TSA must approve the document in order for it to be valid
Approved[1]	Unless used with reference to another person, means approved by TSA.
Apron[2]	A defined area, on a land aerodrome[2], intended to accommodate aircraft for purposes of loading or unloading passengers, mail or cargo, fueling, parking or maintenance.

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

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 for FAA for security-related activities and communications.
ASP	**Airport Security Program**
ASUP	Automated Scene Understanding Program
ATC	Air Traffic Control
ATCT	Airport Traffic Control Tower
ATM	Automated Teller Machine
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. It would not include skycap operations that only accept checked baggage, nor would it include locations performing the same full range of functions but located off the airport.
ATSA	Aviation and Transportation Security Act of 2001
ATSP	Airport Tenant Security Program
Authorized Aircraft Operator Representative[9]	Any individual who is not a direct employee of the aircraft operator but contracted or authorized to act on the aircraft operator's behalf to perform measures required by a security program.
AVSEC	Aviation Security
AVSEC Measures	Aviation Security Contingency Measures
Baggage Claim Area	Space, typically 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
BATF	Bureau of Alcohol, Tobacco and Firearms (U.S.)
BDPH	Busy Day/Peak Hour – Calculation method for screening point peak volume.
BHR	Busy Hour Rate – Calculation method for screening point peak volume.
BHS	Baggage Handling System

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

BIDS	Baggage Information Display Systems
BMA	Baggage Makeup Area
Boarding Gate	That area from which passengers directly enplane or deplane the aircraft.
BOCA	Building Officials Code Authority
Bomb Appraisal Officer[9]	A TSA employee designated and approved by TSA HQ to assist the screening supervisor to determine if checked baggage is or contains an improvised explosive device
BW[10]	Biological weapon (or Biological Warfare)
CAD	Computer-Aided Dispatch
CAPPS	Computer-Assisted Passenger Pre-Screening System
Cargo[1]	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. Aircraft operator security programs further define the term "cargo."
Cargo[2]	Any property carried on an aircraft other than mail, stores and accompanied or mishandled baggage.
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[9]	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
Caution Statement[9]	A written indication of a potentially hazardous situation, which if not avoided, may result in equipment damage
C/B[10]	Chemical/Biological
CBP	Customs and Border Protection (U.S.)
CBRN	Chemical, Biological, Radiological, Nuclear
CBW[10]	Chemical and Biological Weapon (or Chemical and Biological Warfare)
CCC	CBP Coordination Center located within the FIS area.
CCD	Charge-coupled Device
CCTV	Closed Circuit Television (System)
CDC[10]	Center for Disease Control and Prevention

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

Certificate Holder	An aircraft operator subject to 49 CFR 1544 holding an FAA operating certificate and engaged in scheduled passenger or public charter passenger operations (or both). The term is also sometimes applied to a "certificated airport", which refers to an airport's operational certification by FAA pursuant to 14 CFR 139
Certificate Holder[3]	The holder of an Airport Operating Certificate issued by FAA under 14 CFR 139.
CFR	Code of Federal Regulations (U.S.)
Challenge Procedures	
CHRC	Criminal History Records Check
Checked Baggage[1]	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
Checked Baggage[9]	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[10]	Chemical and Biological
CMOS	Complimentary Metal-Oxide Semiconductor
Comm Center	Communications Center
Concourse	A passageway for persons between the principal terminal building waiting area and the structures leading to aircraft parking positions.
Contingency Measures	**AVSEC Measures**
Covered Person[1]	Any organization, entity, individual, or other person described in 49 CFR 1520.7. In the case of an individual, *covered person* includes any individual applying for employment in a position that would be a covered person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. *Covered person* includes a person applying for certification or other form of approval that, if granted, would make the person a covered person described in §1520.7
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.
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

CSS	Checkpoint Screening Supervisor
Curbside Check-in	An area normally located along 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 aircraft more directly.
CUPPS	Common-Use Passenger Processing Systems
CW[10]	Chemical Weapon (or Chemical Warfare)
DFO	Director of Field Operations (CPB)
DHS[1]	The Department of Homeland Security (U.S.) and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.
Direct Operator Employee[9]	A person employed and paid directly by the aircraft operator
Disabling chemicals and other dangerous items	A category of weapons that includes items that may be used for self-defense such as tear gas, pepper spray, and certain household cleaners and other chemicals
DOD	Department of Defense (U.S.)
DOE	Department of Energy (U.S.)
DOT[1]	The Department of Transportation (U.S.) and any operating administration, entity, or office within the Department of Transportation, including the Saint Lawrence Seaway Development Corporation and the Bureau of Transportation Statistics.
Downstream	Colloquial expression usually denoting the area of the airport protected by the security screening checkpoint and/ or access control systems.
DVR	Digital Video Recorder
ECAC	European Civil Aviation Conference
EDS	**Explosives Detection System**
EIA	Electronics Industry Alliance
Emergency Amendment (EA)[6]	An amendment to the security program issued when there is a finding that an emergency requiring immediate action with respect to safety and security in air transportation makes normal regulatory procedures contrary to the public interest
EMD	Enhanced Metal Detector
EMS	Emergency Medical Services
EOC	Emergency Operations Center (See also **Airport Emergency Command Post**)

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

EOD	**Explosive Ordnance Disposal** - To render safe either improvised or manufactured explosive devices by the use of technically trained and equipped personnel.
Escort[1]	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"
ETP	Explosives Trace Portal
EVIDS	Electronic Visual Information Display Systems
Exclusive Area[1]	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[1]	An agreement between the airport operator and an aircraft operator or a foreign air carrier that has a security program under 49 CFR 1544 or 49 CFR 1546 that permits such an aircraft operator or foreign air carrier to assume responsibility for specified security measures in accordance with 49 CFR 1542.111.
Explosive or Explosive Device[1]	Includes, but is not limited to, an explosive or explosive material as defined in 18 U.S.C. 232(5), 841(c) through 841(f), and 844(j), and a destructive device as defined in 18 U.S.C. 921(a)(4) and 26 U.S.C. 5845(f).
Explosives[9]	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 against pre-established standards, and has certified that the system meets the criteria in terms of detection capabilities and throughput
Explosives Detection System[9]	A TSA certified automated device, or combination of devices, which has the ability to detect in checked baggage, the amounts, types, and configurations of explosive materials as specified by TSA
Explosives Trace Detection[9]	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
Explosives Trace Detector	As used in this document, a device that detects tiny amounts of particle and/or vapor forms of explosives
FAA[1]	Federal Aviation Administration (U.S.)
FAC	Family Assistance Center

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

FAM	TSA Federal Air Marshal
FAR	Federal Aviation Regulation (U.S.)
FBI	Federal Bureau of Investigation (U.S.)
FBO	Fixed Base Operator
fc	Footcandle
FCC	Federal Communications Commission (U.S.)
FDA	Food and Drug Administration (U.S.)
Federal Flight Deck Officer[1]	A pilot participating in the Federal Flight Deck Officer Program under 49 U.S.C. 44921 and implementing regulations
FEMA	Federal Emergency Management Agency (U.S.)
FIDS	Flight Information Display Systems
Firearm[9]	Any weapon, including a starter gun and antique firearm, that will or is designed to or may readily be converted to expel a projectile by action of an explosive, or the frame or receiver of any such firearm
Firearm or Other Weapon[1]	Includes, but is not limited to, firearms as defined in 18 U.S.C. 921(a)(3) or 26 U.S.C. 5845(a) or items contained on the U.S. Munitions Import List at 27 CFR 447.21
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)
Flightcrew Member[1]	A pilot, flight engineer, or flight navigator assigned to duty in an aircraft during flight time
Flight School Employee[1]	A flight instructor or ground instructor certificated under 14 CFR Part 61, 141, or 142; a chief instructor certificated under 14 CFR Part 141; a director of training certificated under 14 CFR Part 142; or any other person employed by a flight school, including an independent contractor, who has direct contact with a flight school student. This includes an independent or solo flight instructor certificated under 14 CFR Part 61
FOIA[10]	Freedom of Information Act
FSD	TSA Federal Security Director
FSR	Full-Scale Range
FWS	Fish and Wildlife Service (U.S.)
G8	Group of 8 (Nations)
GA	**General Aviation**

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

General Aviation	That portion of civil aviation that encompasses all facets of aviation except aircraft operators holding a Certificate of Conveyance and Necessity from the FAA and large aircraft commercial operators.
GSEM	Ground Services Equipment Maintenance (Facility)
GSC	Ground Security Coordinator, that aircraft operator official required to perform certain security duties and responsibilities as defined by 49 CFR 1544
Ground Transportation Staging Area	The location where taxis, limos, buses and/or other ground transportation vehicles are staged prior to the terminal.
GTSA	**Ground Transportation Staging Area**
Hazardous Material[1]	As defined in 49 USC 5103 et seq. of the hazardous materials transportation law.
Hazardous Materials[9]	Substances or materials that have been determined to be capable of posing an unreasonable risk to health, safety, and property when transported in commerce, and which have been so designated under the HMR. Hazardous materials are also referred to as "dangerous goods" under international regulations
HID	High-Intensity Discharge
Hijacking	The exercising, or attempt to exercise, control over the movement of an aircraft by the use of force, threats, or other actions, which if successfully carried out, would result in the deviation of an aircraft from its regularly scheduled route.
HSAS	Homeland Security Advisory System
Hub	An airline terminal and airport used to transfer passengers to and from a large number of connecting flights.
HVAC	Heating, Ventilation and Cooling
IATA	International Air Transport Association
IAB	International Arrivals Building
IBC	International Building Code
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.
ICBO	International Conference of Building Officials
IC	Information Circular
ICE	DHS Immigration and Customs Enforcement

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

ID	Identification - use of methods such as access media, signs or markers to identify persons, vehicles and/or property
IDF	Intermediate Distribution Facility (Frame)
IED	**Improvised Explosive Device**
IEEE	Institute of Electrical and Electronic Engineers
IESNA	Illumination Engineering Society of North America
IETF	Internet Engineering Task Force
Information Circular[6]	A document issued by the TSA Transportation Security Intelligence Service (TSIS) that formally transmits information concerning threats to industry personnel who have the operational need to know and can take appropriate action
Improvised Explosive Device[9]	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).
Incendiary[9]	Any substance or device that can be used to initiate a fire.
Index[3]	The type of aircraft rescue and firefighting equipment and quantity of fire extinguishing agent that the certificate holder must provide in accordance with §139.315
Indirect Air Carrier[1]	Any person or entity within the United States not in possession of an FAA air carrier operating certificate that undertakes to engage indirectly in air transportation of property, and uses for all or any part of such transportation 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)[6]	A standard security program for indirect air carriers regulated in accordance with 49 CFR 1548
Integrated systems	An EDS whose baggage feed and output belts are directly connected to an airline's baggage belt system. Baggage is introduced into the EDS without manual loading or unloading by TSA screeners
Interline Baggage	Baggage of passengers subject to transfer from the aircraft of one operator to the aircraft of another in the course of the passenger's travel.
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).

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

International Airport[2]	Any airport designated by the Contracting State[2] in whose territory it is situated as an airport 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
IP	Internet Protocol
IR	Infrared
IS	Information Systems
ISC	In-flight Security Coordinator, that aircraft operator official (pilot in command of an aircraft) required to perform certain security duties and responsibilities as defined by 49 CFR 1544
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.
IT	Information Technology
ITU	International Telecommunications Union
Joint-Use Airport[3]	An airport owned by the United States that leases a portion of the airport to a person operating an airport specified under § 139.1(a)
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
Law Enforcement Officer[9]	A sworn employee of a government entity (Federal, State, and local, including U.S. military police) with full power of arrest, who is trained and commissioned to enforce the public criminal laws of the jurisdiction(s) in which he or she is commissioned.
Landside[2]	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.)
LBNL[10]	Lawrence Berkeley National Laboratory
Lead Screener[9]	A screener who is designated by TSA management or a screening supervisor to perform additional duties and responsibilities. A lead screener may be designated to perform functions of a screening supervisor. In this SOP, when the term screening supervisor is used, it also refers to a lead screener designated to perform supervisory functions

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

LED	Light-Emitting Diode
LEO	**Law Enforcement Officer**
Loaded Firearm[1]	A firearm that has a live round of ammunition, or any component thereof, in the chamber or cylinder or in a magazine inserted in the firearm
LSZ[10]	Life Safety Zone
LVIED	Large Vehicle IED
MAC	Medium Access Control (LAN)
MDF	Main Distribution Facility (Frame)
Metal Detector **[also: "magnetometer"]**	An electronic detection device approved for use by the FAA to detect metal on the person of people desiring access beyond the screening point. May be walk-through or hand-held type.
micron	0.001 Millimeter or 0.00004 inches
Mobility Aid[9]	A device or assistance mechanism used by a person with a disability to aid in his or her mobility such as a cane, crutches, or an animal
Movement Area[2]	That part of an aerodrome[2] to be used for the take-off, landing and taxing or aircraft, consisting of the maneuvering area and the apron(s).
Movement Area[3]	The runways, taxiways, and other areas of an airport that are used for taxiing, takeoff, and landing of aircraft, exclusive of loading ramps and aircraft parking areas.
MPV	Maximum Peak Volume
MTF	Modulation Transfer Function
NAS	Network Attached Storage
NAVAID	Navigational Aid
NCIC	National Crime Information Center (U.S.)
NEC	National Electrical Code
NFPA	National Fire Protection Association (U.S.)
NIOSH[10]	National Institute for Occupational Safety and Health
NIST	National Institute of Standards and Technology (U.S.)
Non-restricted Area[2]	Areas of an airport to which the public have access or to which access is otherwise unrestricted
NQR	Nuclear Quadropole Resonance
O&D	Origin & Destination – Airport operational type (as opposed to Transfer/Hub)

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

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[9]	EDS tools/functions that can be used to resolve or suspect EDS alarm objects
Operator[2]	A person, organization or enterprise engaged in or offering to engage in an aircraft operation.
OUO[10]	Official Use Only (OUO) information
Passenger Area[2]	All the ground space and facilities provided for passenger processing. It includes aprons, passenger buildings, vehicle parks and roads
Passenger Seating Configuration[1]	The total maximum number of seats for which the aircraft is type certificated that can be made available for passenger use aboard a flight, regardless of the number of seats actually installed, and includes that seat in certain aircraft that may be used by a representative of the FAA to conduct flight checks but is available for revenue purposes on other occasions
PBFM	Passenger and Baggage Flow Model
PCII	Protected Critical Infrastructure Information
PDA	Portable Digital Assistance
PDS	Premise Distribution System
PDU	Power Distribution Units
Perimeter	The outer boundary of an airport, also a boundary that can separate areas controlled for security purposes from those that are not.
Person[1]	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.
PHS	Public Health Service (U.S.)
PHY	Physical Layer
PIN	Personal Identification Number
POE	Port-of-Entry (FIS).
PPL	Primary Processing Lane(s) (FIS)
Post Check-in Screening[9]	Checked baggage screening that occurs after the passenger checks in at the aircraft operator's ticket counter, including curbside
Pre-Check-in Screening[9]	Checked baggage screening that occurs before the passenger checks in at the aircraft operator's ticket counter, including curbside

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

Private Charter[1]	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
PROACT[10]	Protective and Responsive Options for Airport Counter-Terrorism
Prohibited Items[9]	Items that cannot be transported in checked baggage
PROTECT[10]	Program for Response Options and Technology Enhancements for Chemical/Biological Terrorism
PSS	Physical Security System
PTZ	Pan/Tilt/Zoom
Public Area	That portion of the airport which includes all public real estate and facilities other than the air operations area and those sterile areas downstream of security screening stations
Public Charter[1]	Any charter flight that is not a private charter
RAID	Random Array of Inexpensive Disks
Record[1]	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
Sabotage	The intentional and willful damage or destruction of civil aviation-related goods or property, either on the ground or in the air.
Safety Area[3]	A defined area comprised of either a runway or taxiway and the surrounding surfaces that is prepared or suitable for reducing the risk of damage to aircraft in the event of an undershoot, overshoot, or excursion from a runway or the unintentional departure from a taxiway
SAFTI	Secure and Facilitated International Travel Initiative
SAN	Storage Area Network

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

SARPS	Standards and Recommended Practices (ICAO)
SBCCI	Southern Building Code Congress International
SBR	Standard Busy Rate – Calculation method for screening point peak volume.
Scheduled Operation[3]	Any common carriage passenger-carrying operation for compensation or hire conducted by an air carrier for which the air carrier or its representatives offers in advance the departure location, departure time, and arrival location. It does not include any operation that is conducted as a supplemental operation under 14 CFR Part 121 or public charter operations under 14 CFR Part 380
Scheduled Passenger Operation[1]	An air transportation operation (a flight) from identified air terminals at a set time, which is held out to the public and announced by timetable or schedule, published in a newspaper, magazine, or other advertising medium
Screener[9]	Any individual who is authorized to inspect individuals and/or property for the presence of explosives, incendiaries, weapons, or other prohibited items
Screening[2]	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
Screening Function[1]	The inspection of individuals and property for weapons, explosives, and incendiaries
Screening Functions[9]	The checked baggage screening functions are: (1) EDS screening, (2) ETD screening, (3) combination of EDS/ETD, and (4) physical inspection
Screening Location[1]	Each site at which individuals or property are inspected for the presence of weapons, explosives, or incendiaries
Screening Location[9]	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
Screening Supervisor[9]	The individual who directly supervises screeners and the screening process. At some airports, a lead screener may be designated to perform functions of a screening supervisor. In this SOP, when the term screening supervisor is used, it also refers to a lead screener designated to perform supervisory functions
SD	Security Directive
Secured Area[1]	A portion of an airport, specified in the airport security program, 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.

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

Security Areas	Areas defined by and subject to security requirements and regulation; e.g. AOA, ATSP Area, Exclusive Area, Secured Area, SIDA, Sterile Area
Security Restricted Area[2]	Those areas of the airside of an airport which are identified as priority risk areas where in addition to access control, other security controls are applied. Such areas shall normally include, inter alia, all commercial aviation passenger departure areas between the screening checkpoint and the aircraft, the ramp, baggage make-up areas, including those where aircraft are being brought into service and screened baggage and cargo are present, cargo sheds, mail centers, airside catering and aircraft cleaning premises
Security Contingency Plan[1]	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[6]	A document issued by TSA to notify aircraft operators and/or airport operators of specific credible threats
Security Identification Display Area[1]	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 the secured area and may include other areas of the airport.
Security Program[1]	A program or plan and any amendments, developed for the security of the following, including any comments, instructions, or implementing guidance: (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 Programme[2]	Measures adopted to safeguard international civil aviation against acts of unlawful interference.
Security Parking Area	An aircraft stand where aircraft threatened with unlawful interference may be parked pending resolution of the threat. Also known as “hot spot”
Security Screening[1]	Evaluating a person or property to determine whether either poses a threat to security.
Selectee[9]	A person selected for additional screening by a computer-assisted passenger prescreening system or another process as determined and approved by TSA
Selectee Screening[9]	A special screening requirement for individuals selected by a computer-assisted passenger prescreening system or another process as determined and approved by TSA
Shared-Use Airport[3]	A U.S. Government-owned airport that is co-located with an airport specified under § 139.1(a) and at which portions of the movement areas and safety areas are shared by both parties
Shield Alarm[9]	An EDS alarm caused by substances too dense for x-rays to penetrate. The result is a suspect volume, which EDS is unable to analyze

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section ‘D’ Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

Should	For the purpose of this document, this word is defined as a recommendation or that which is advised but not required.
SIDA	**Security Identification Display Area**
SNL[10]	Sandia National Laboratories
SOC	Security Operations Center
SONET	Synchronous Optical Network
Special Statutory Requirement To Operate to or From a Part 139 Airport[3]	Each air carrier that provides—in an aircraft designed for more than 9 passenger seats—regularly scheduled charter air transportation for which the public is provided in advance a schedule containing the departure location, departure time, and arrival location of the flight must operate to and from an airport certificated under part 139 of this chapter in accordance with 49 U.S.C. 41104(b). That statutory provision contains stand-alone requirements for such air carriers and special exceptions for operations in Alaska and outside the United States. Certain operations by air carriers that conduct public charter operations under 14 CFR Part 380 are covered by the statutory requirements to operate to and from 14 CFR Part 139 airports. See 49 U.S.C. 41104(b)
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[1]	Sensitive security information, as described in §1520.5
Stand-Alone Systems[9]	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[1]	A portion of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an aircraft operator under 49 CFR 1544 or a foreign air carrier under 49 CFR 1546, through the screening of persons and property.
Sterile Area[2]	That area between any passenger inspection or screening control point and aircraft into which access is strictly controlled. (Also known as Security restricted area.)
Sterile Area[9]	A portion of an airport that provides individuals access to boarding aircraft and to which access is generally controlled by TSA through the screening of persons and property.
Suspect Bag/Item[9]	A bag or item that alarms an EDS/ETD for which the cause of the alarm cannot be cleared with alarm resolution procedures
Taxiway	A paved surface over which aircraft taxi to and from a runway, a hangar, etc.
TCU	Threat Containment Unit - any of a wide variety of devices intended to be 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.

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

TDMM	Telecommunications Distributions Methods Manual
Terminal	A building or buildings designed to accommodate the enplaning and deplaning activities of aircraft operator passengers.
T/H	Transfer/Hub
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 under take actions that would be detrimental to U.S. interest. There are six primary sources of threats: Terrorist, Criminal, Insider, Foreign Intelligence Service, Foreign Military, Environmental; as defined by the CIA's Analytical Risk Management Program
Threat[8]	The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operations
Threat Image Projection System[1]	An evaluation tool that involves periodic presentation of fictional threat images to operators and is used in connection with x-ray or explosives detection systems equipment
TIA	Telecommunications Industry Association
TMS	Terminal Management System
TPHP	Typical Peak Hour Passengers – Calculation method for screening point peak volume.
Transportation Security Regulation(s)[1]	The regulations issued by the Transportation Security Administration, in title 49 of the Code of Federal Regulations, chapter XII, which includes parts 1500 through 1699
TSA[1]	Transportation Security Administration (U.S.)
TSA Cleared Sticker[9]	A numbered, adhesive tag provided by TSA that is affixed to checked baggage tags after each bag has been cleared for transport
TSA Management[9]	The FSD or FSD designate who has overall responsibility for the screening locations at an airport
49 CFR	Transportation Security Regulations
TV	Television
TWIC	Transportation Workers Identification Card
UBC	Uniform Building Code
UK	United Kingdom
Unescorted Access Authority[1]	The authority granted by an airport operator, an aircraft operator, foreign air carrier, or airport tenant under part 1542, 1544, or 1546, to individuals to gain entry to, and be present without an escort in, secured areas and SIDAs of airports

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

United States[1]	In a geographical sense, means the States of the United States, the District of Columbia, and territories and possessions of the United States, including the territorial sea and the overlying airspace
Unscheduled Operation[3]	Any common carriage passenger-carrying operation for compensation or hire, using aircraft designed for at least 31 passenger seats, conducted by an air carrier for which the departure time, departure location, and arrival location are specifically negotiated with the customer or the customer's representative. This includes any passenger-carrying supplemental operation conducted under 14 CFR Part 121 and any passenger-carrying public charter operation conducted under 14 CFR Part 380
U.S.	United States
UPS	Uninterruptible Power Supply
USPS	United States Postal Service
UTP	Unshielded Twisted Pair
VAC	Volts Alternating Current
VLAN	Virtual Local Area Network
VOIC	Voice of Internet Protocol
Vulnerability[5]	. . . a weakness in physical structures, personnel protection systems, process or other areas that may be exploited by terrorists . . .
Vulnerability Assessment[1]	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	Any facility or area on or connected with an airport, which, if damaged or otherwise rendered inoperative would seriously impair the functioning of an airport.
Vulnerable Point[2]	Any facility on or connected with an airport, which, if damaged or destroyed, would seriously impair the functioning of the airport
VPN	Virtual Private Network
Warning Statement[9]	A written indication of a potentially hazardous situation, which if not avoided, could result in personal injury or occupational illness
WAM	Workforce Analysis Model
WAN	Wide-Area Network

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

WLAN	Wireless Local Area Network
WMD	Weapon of Mass Destruction
WMD[10]	Weapons of Mass Destruction (typically includes chemical, biological, radiological, and nuclear weapons)
WTMD	Walk-Through Metal Detector

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

THIS PAGE INTENTIONALLY LEFT BLANK

[1]Defined by 49 CFR Parts 1500, 1520, 1540, 1552, 1572 - [2]Defined by ICAO Annex 17 - [3]Defined by 14 CFR Part 139 - FAA Airport Certifications - [4]Airport Improvement Program Handbook FAA - [5]GAO 02-150T - [6]TSA Pertinent Policy Definitions - [7]TSA Inspection Glossary - [8]Interagency OPSEC Glossary of Terms – [9]Section 'D' Specific Screening Definitions – [10]Sandia Report, Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism

APPENDIX F

BIBLIOGRAPHY

NOTE:

DHS, TSA, FAA and other sources/agencies listed below periodically update many of the documents referenced in this bibliography, as well as many rules, regulations, statutes and codes. These updates sometimes change the entire document, but more often the changes are only in segments as new information becomes available. The reader should be certain when seeking guidance from such referenced documents that he/she is obtaining the most current version from the source.

Section A - 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 internet web site at *www.faa.gov*]

1. 00-2, Advisory Circular Checklist - Contains a listing of all current advisory circulars.

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 Advisory Circular still exists for operational guidance for foreign air carriers only.

3. 150/5200-31A, Airport Emergency Plan

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

Section B - Government Reports and Regulations

Government reports may be obtained from the National Technical Information Services (NTIS). Springfield, Virginia 22151. In general, they may also be obtained from the originating government agency, and they are often also available on the agency's internet web site.

1. Aircraft Hijacking and Other Criminal Acts against Civil Aviation -- Statistical and Narrative Reports. Office of Civil Aviation Security, Federal Aviation Administration, issued annually.

2. Aviation and Transportation Security Act (ATSA). Public Law 107-71. 115 Statute 597.

3. Criminal Acts against Civil Aviation (current year). Office of Civil Aviation Security, Federal Aviation Administration, issued annually.

4. 49 CFR 1520. Protection of Sensitive Security Information

5. 49 CFR 1540. Civil Aviation Security General Requirements.

6. 49 CFR 1542. Airport Security.

7. 49 CFR 1544. Aircraft Operator Security.

8. 49 CFR 1546. Foreign Air Carrier Security.

9. 49 CFR 1548. Indirect Air Carrier Security.

10. 14CFR139, Certification and Operations: Land Airports Serving Certain Air Carriers

11. Homeland Security Act, Public Law 107-296.

Section C - 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)

1. Airport Planning Manual - Master Planning, Part 1. International Civil Aviation Organization.

www.icao.int

2. Aviation Security Improvement Act of 1990. PL 101-604. Federal Aviation Administration.

3. Crisis Management Manual, Transportation Security Administration.

4. Transit Security Design Considerations, Final Report, John A. Volpe National Transportation Systems Center, U.S. Department of Transportation, November 2004.

5. DoD Minimum Antiterrorism Standards for Buildings, U.S. Department of Defense, October 2003.

6. Physical Security. U.S. Army FM 3.19.30, January 2001.

http://www.wbdg.org/ccb/ARMYCOE/FIELDMAN/fm31930.pdf

7. Existing and Potential Standoff Explosives Detection Techniques, 2004, Board of Chemical Sciences and Technologies, The National Academies Press, 2004 Available for purchase at:

www.nap.edu/books/0309091306/html/12.html

8. Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism, Sandia Berkley National Laboratory, SAND2005-3237/LBNL-54973 (II), May 2005, prepared for the U.S. Department of Energy

http://www.sandia.gov/news-center/news-releases/2005/images/unlsand-2005-3237.pdf

9. Handbook for Security Glazing. Naval Facilities Engineering Command.

10. Glazing Hazard Mitigation, Applied Research Associates, Inc.

http://www.wbdg.org/design/glazingmitigation.php

11. 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.

12. 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/

13. International Standards and Recommended Practices – Security - Safeguarding International Civil Aviation Against Acts of Unlawful Interference - Annex 17 to the Convention on International Civil Aviation. International Civil Aviation Organization. Available for purchase from:

http://www.icao.int/

14. National Fire Codes NFPA 101 - Life Safety Code. National Fire Prevention Association. Available for purchase from:

www.nfpa.org

15. National Fire Codes NFPA 416 - Standard on Construction and Protection of Airport Terminal Buildings. National Fire Prevention Association. Available for purchase from:

www.nfpa.org

16. National Fire Codes NFPA 417 - Standard on Construction and Protection of Aircraft Loading Walkways. National Fire Prevention Association. Available for purchase from:

www.nfpa.org

17. Merritt Risk Management Manual, available for purchase from Silver Lake Publishing at:

www.riskmanagementmanual.com/index.php

18. RTCA/DO-230, Standards for Airport Security Access Control Systems.

19. Security Guidelines for General Aviation Airports. Aviation Security Advisory Committee.

http://www.tsa.gov/interweb/assetlibrary/security_guidelines_for_general_aviation_airports_may_2004_a-001.pdf

20. Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference. International Civil Aviation Organization. Available for purchase from:

http://www.icao.int/

21. Terrorism in the United States - Terrorist Research and Analytical Center. Counter Terrorism Section, Criminal Investigative Division. Federal Bureau of Investigation. Annual.

http://www.fbi.gov/publications/terror/terroris.htm

22. Vulnerability Identification Self Assessment Tool (VISAT), Transportation Security Administration, U.S. Department of Homeland Security

www.tsa.gov/public/interapp/tsa_policy/tsa_policy_0045.xml

23. DOE Vulnerability and Risk-Assessment Methodology, Vulnerability and Risk Management Program, U.S. Department of Energy, 2001

www.esisac.com/publicdocs/assessment_methods/AppD_DOE_VRAP.pdf

24. Lessons Learned from Industry Vulnerability Assessments and September 11th, a presentation of Argonne National Laboratory, U.S. Department of Energy, December 2001

www.naseo.org/committees/energysecurity/energyassurance/stern.pdf

25. The Public Transportation System Security and Emergency Preparedness Planning Guide, DOT-FTA-MA-26-5019-03-01, Federal Transit Administration, U.S. Department of Transportation, January 2003

www.transit-safety.volpe.dot.gov/Publications/security/PlanningGuide.pdf

26. A How-To Guide Mitigate Potential Terrorist Attacks Against Buildings, FEMA 452, January 2005, Federal Emergency Management Agency, U.S. Department of Homeland Security

www.fema.gov/

27. Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks, FEMA 427, December 2003, Federal Emergency Management Agency, U.S. Department of Homeland Security

www.fema.gov/fima/rmsp427.shtm

28. Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, FEMA 426, December 2003, Federal Emergency Management Agency, U.S. Department of Homeland Security

www.fema.gov/

29. The Design and Evaluation of Physical Protection Systems, Mary Lynn Garcia, published by Butterworth-Heinemann, 2001. Available for purchase at Internet book sites.

30. Progressive Collapse Analysis and Design Guidelines for New Federal Office Buildings and Major Modernization Projects, U.S. General Services Administration, June 2003

http://www.oca.gsa.gov/software/about_progressive_collapse/progcollapse.php

31. Chain Link Fence Manufacturers Institute Security Fencing Recommendations, Chain Link Fence Manufacturers Institute, posted on its web sites:

www.chainlinkinfo.org and *http://www.associationsites.com/page.cfm?pageid=887&usr=clfma*

Section D - 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) *www.uscis.gov/graphics/lawsregs/ina.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 Code of Federal Regulations (CFR): International Airports for Entry of Aliens.

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.

HSPD -12- Addresses information technology 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

4. 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.

5. 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/xp/cgov/travel/inspections_carriers_facilities/fis.xml

6. Lessons Learned in Terminal Design –Post 9/11, International Airlines Building (Federal Inspection Station) George Bush Intercontinental Airport, a presentation by Col. Eric R. Potts (Ret.), Deputy Director Planning, Design & Construction, Houston Airport System, 2005

www.aci-na.org/docs/41%20SAN%2005%20Eric%20Potts%20Terminal%20Design%20Post%209%2011.pdf

Section E - Miscellaneous Regulations and Reports

1. Guidelines for Airport Signing and Graphics, Apple Designs, Inc., available for purchase from its web site: www.appledesigns.net FAA Circular 150/5360-12D, dated July 1, 2003 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.

www.usdoj.gov/crt/ada/stdspdf.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 web sites:

www.osha.gov/SLTC/ergonomics

www.osha.gov/SLTC/etools/baggagehandling/index.html

www.osha.gov/SLTC/etools/computerworkstations/components_monitors.html

APPENDIX G

REPORT CARD FOR AIRPORT CHEM-BIO PROTECTION AND RESPONSE

Information in this appendix is from Edwards, Dr. Donna M., *et al*, "Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism," Sandia Report SAND2005-3237, Berkeley Lab Report LBNL-54973 (May 2005), Prepared by Sandia National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550.

Give a letter grade **(A+ to F)** for each item. Score each building separately where appropriate.

SECURITY DOESN'T COME FROM A GRADE! This scorecard will give a rough idea where you stand; it's no substitute for common sense, thoughtful planning, and realistic practice.

Priority I:

____ Prevent access to building air intakes and HVAC mechanical rooms

An A+ grade requires that all building air intakes and HVAC mechanical rooms are completely inaccessible to unauthorized personnel, including airport employees, even if tools are employed (e.g. ladders to scale walls, lockpicks or sledgehammers to open doors); this can be attained by using intrusion alarms, security cameras, etc., in addition to physical barriers.

____ Train airport employees to recognize and respond to Chem-Bio attacks

Training should include an annual drill, and should cover: Recognizing chem-bio delivery devices; Recognizing signs of chemical attacks, including symptoms, odors, etc.; immediately selecting an appropriate response area; initiating evacuation or shelter-in-place as needed; initiating HVAC response; detaining people if necessary; and initiating "tracking" potential victims via passenger manifests.

____ Establish and practice evacuation procedures

Train personnel to assess the size of the area that needs to be evacuated; assess evacuation routes for safety; immediately initiate evacuation using safe routes; establish methods for segregating exposed and unexposed people; establish collection and treatment areas where people will assemble for triage and treatment.

____ Establish procedures to analyze contamination and decontaminate exposed people

Perform decontamination planning and training with airport police, airport firefighters, local hazardous materials teams, and others, and establish procedures for sampling and testing potential biological agent and for identifying and decontaminating exposed people.

____ Create airflow isolation to reduce spread of contamination between buildings or zones

(1) Required to get an "A" on this item: Install physical barriers that eliminate air exchange between zones. For instance, each gate or group of adjacent gates might be separated from the mezzanine by a glass wall, with sliding doors that allow access. This arrangement is highly beneficial *only if* the enclosed spaces have HVAC systems that do not mix air with other areas.

(2) If there are no physical barriers between zones, then to get a "B" on this item: Pressure-balance the HVAC system to minimize air flows between isolation zones (which may be entire buildings). This will provide some benefit even if there are no physical barriers between isolation zones.

(3) Install fire doors or other air barriers that can be triggered remotely in the event of a chemical or biological attack. The more zones that can be isolated in this way, the better.

Priority II:

____ Protect critical emergency response functions by providing clean air

(1) Operate HVAC so as to pressurize critical non-public areas. This will prevent or slow the spread of agent from public to non-public areas, and so will help protect the people controlling the emergency response, but will not directly protect the public at large.

(2) Air handling units that serve critical areas (such as security offices) should not provide air that is mixed with re-circulated air from public areas.

____ Install and maintain highly effective HVAC filters

Ideally, filters should meet or exceed the ASHRAE standard for MERV-12 filters, should be replaced on a regular schedule, and should be checked regularly for filter "bypass" (that is, to make sure air can't sneak around the filters rather than pass through them).

____ Enable and test remote emergency airflow command and control

The HVAC system should be controllable remotely (including bathroom and food court exhaust fans). HVAC and exhaust fans should have rapid shutdown capability (ideally within 2 minutes of initiation). Test dampers and fans to make sure they respond to remote commands. Remote control system must be secure against unauthorized use.

____ Establish procedures to "shelter in place" during an outdoor attack

Pre-identify "shelter in place" areas; assign responsibilities to close interior and exterior doors; create a chain of command for shutting off HVAC and closing dampers.

____ Establish procedures to segregate and detain people if quarantine is needed

Pre-identify areas where people can be detained and can be segregated by likely exposure (none/unknown/exposed, or none/possible). Assign responsibilities and procedures for rapidly moving people out of contaminated areas without bringing them in contact with unexposed people.

Priority III:

____ Prevent or reduce access to return air grilles

Easy public access to return air grilles can allow chemical or biological agents to be introduced to the HVAC system. Reduce access by elevating grilles where possible, by moving them (or moving other objects) to make them visible to airport personnel, or by using barriers to prevent access.

____ Prevent or reduce access to HVAC relief/exhaust grilles

In many systems HVAC exhausts sometimes act as supply units: air is pulled into the building rather than expelled. Reduce access by elevating them, moving them to make them more visible, or by using barriers to prevent access.

____ Provide video monitoring capability to quickly identify/monitor affected areas

Video monitoring with good coverage of occupied areas can help diagnose an attack quickly, identify the magnitude of the problem, and select safe evacuation routes.

____ Prevent access to building information (HVAC blueprints, etc.)

Building information can allow terrorists to maximize the effectiveness of their attack. Retrieve blueprints and plans from contractors when feasible.

____ Establish procedures to detect covert biological attack

If a bio attack is anticipated, perform regular testing of ventilation filters or install special bio sensors. Monitor employee absenteeism for evidence of sudden illness.