Recommended Security Guidelines for Airport Planning, Design and Construction

Transportation
Security
Administration

Revised: May 2011

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 providing information exchange to enhance the planning and design of airport security systems. The U.S. Government assumes no liability for the contents or use. This document does not create regulatory requirements or mandates of any kind. 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, alternatives, 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 TSA Internet site: http://www.tsa.gov

Or contact the security staff person 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

ACKNOWLEDGEMENTS

This document is intended to bring to the attention of the airport planning, design, and engineering community the serious security concerns that should 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 broad experience of the community and will help the reader anticipate future expansion needs.

To complete this fourth revision of the document, an Aviation Security Advisory Committee (ASAC) Working Group was formed. Under the auspices of this working group, over 100 persons attended meetings, contributed to the development of various drafts and participated in document reviews. A few participants, referred to as Section Chiefs, chaired team meetings and 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 should 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, Transportation Security Administration (TSA), who proposed creation of the working group and supported this project from start to finish as Co-chair;

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

Dawn E. Lucini, TSA, Transportation Sector Network Management (TSNM), who administered the project and internal TSA efforts from its inception;

Chris Runde, TSA, TSNM, who co-administered the project from the TSA perspective and saw to it that requests for Agency inputs were fulfilled;

Jose Chaves, TSA, TSNM, who coordinated internal TSA efforts and facilitated other participating Agencies' and industry submittals;

Art Kosatka, TranSecure Inc., the Project Manager, organizer, and principal editor; and

Nancy Hill Ward, TranSecure Inc., who was the Project Administrator, co-editor of every chapter, and did the great bulk of structural work in transitioning the document from the old version to the new.

Guidelines Section	**Section Chiefs**
Cover Art, graphics	Ed Croft, BWI Airport; J. Leonard Wood, Condor Aviation
Part II, Planning and Design	Alex Seid, Parsons; Dave McGhee, Ross & Baruzzini
Part III, Section A, Airport Layout & Boundaries	Charles Cinquemani, DFW Airport; Jorge Reis-Filho, PANYNJ
Part III, Section B, Airside	David Pollard, Tallahassee Regional Airport; Tim Skinner, Lihue Airport (HI)
Part III, Section C, Landside	David Pollard, Tallahassee Regional Airport; Tim Skinner, Lihue Airport (HI)
Part III, Section D, Terminal-Cargo	Art Kosatka, TranSecure Inc.
Part III, Section E, Baggage Screening	Theresa Coutu, Leigh-Fisher
Part III, Section F, Passenger Screening	Scot Thaxton, TSA
Part III, Section G, Access Control (ACAMS)	Christer Wilkinson, AECOM; Colleen Chamberlain, AAAE
Part III, Section H, Video Surveillance, Detection	James McGuire, TranSecure Inc.
Part III, Section I, IT Power Communications	James McGuire, TranSecure Inc. Enrique Melendez, Paragon
Part IV, APP A, Vulnerability Assessment	Bradley W. Fawsett, TSA FAMS office; Annmarie Jenkins, TSNM Airports Division
Part IV, APP B, Chem-Bio Mitigation	Sandia Laboratories
Part IV, APP C, Blast Mitigation	Terry Palmer, Magnusson Klemencic Assoc.; Michael Beairsto, Arup
Part IV, APP D, General Aviation	Craig Spence, AOPA; Brittney Miculka, AOPA
Part IV, APP E, Planning & Design, Command & Control	Donald Zoufal, SDI
Part IV, APP F, International AVSEC	Kristina Dores, International Civil Aviation Organization (ICAO); Solomon Wong, InterVistas

Chamberlain, Colleen	AAAE
Wilkinson, Christer	AECOM System Solutions
Wechsler, Richard F.	AECOM Systems Solutions
Fisher, Clint	Air Transport Association
Thacker, Eric	Air Transport Association
Miculka, Brittney	AOPA
Hochsteller, Paula	Airport Consultants Council
Reynolds, John	Airport Consultants Council
Kellogg, Lydia	Airports Council Intl- NA
Kilborn, Edgar	Analogic
Matty, Scott	Applied Wireless
Spence, Craig	AOPA
Witkowski, Christopher	Assn. Flight Attendants
Beckman, Lori	Aviation Security Consulting
Stout, Leonard	Bechtel Corp.
Cooney, Thomas	Broward County Aviation
Crain, Ron	Burns & McDonnell
Croft, Ed	BWI Airport
McGuire, Mark	Campbell & Paris Engineers
Olislagers, Robert	Centennial Airport
Bowen, Frank	Columbus Regional Airport
Wood, J. Leonard	Condor Aviation
Bradbury, Nancy	Consultant
Malotky, Lyle	Consultant
Lazarick, Richard	CSC Identity Labs
Roth, Richard	CTI Consulting
Cinquemani, Chas	DFW International Airport
Black, Alan	DFW International Airport
Mazzola, Sal	Faith Group LLC
Boggus, Roddy	Gresham, Smith and Partners
Hellwig, Tom	Gresham, Smith and Partners
Frazier, Jeremiah	Hartsfield-Jackson ATL Intl
Ignacio, Jonathan	Hatch Mott MacDonald
Hyde, R.A.	HNTB Corp.
Kohout, Richard	Homeland Security Institute
Dunlap, Kenneth	IATA
Stewart, David	IATA
Dores, Kristina	ICAO, Kabul, Afghanistan
Hamilton, Walter	ID Technology Partners
Lisimaque, Gilles	ID Technology Partners

Auman, David	ID Technology Partners
Geisler, Patrick	Infrastructure Associates, Inc.
Mann, Michael J.	Infrastructure Associates, Inc.
Baumgardner, R.	Indianapolis Airport Auth.
Burnett, Andrew	Indianapolis Airport Auth.
Novak, George	Intervistas
Wong, Solomon	Intervistas
Cintron, Michael	Int’l Airline Passengers Assn.
Stasher, Denson	Jackson Municipal Airport
Clark, Wayne	Jacksonville Airport Auth.
Studdiford, Larry	Jacobs Engineering
Redhead, Ian	Kansas City Intl Airport
Ferguson, Tony	L1 Identify Solutions
Muscatello, Dan	Landrum & Brown
Coutu, Theresa	Leigh-Fisher Consultants
Skinner, Tim	Lihue Airport (HI)
Staar, Greg	Los Angeles World Airports
Petty, Steve	Louisville Airport
Palmer, Terry	Magnusson Klemencic Assc.
Sleiman, Sam	Massachusetts Port Authority
Keegan, Michael	Milwaukee Gen. Mitchell AP
Howell, Alan	Minneapolis-St. Paul Apts
Anderson, Tim	Minneapolis-St. Paul Apts
Dillard, Rosemary	Nat’l. Air Disaster Alliance
Broyles, Scott	National Safe Skies Alliance
Mellinger, Mark	NW Arkansas Regional Apt
Ashley, Gareth	Ove Arup and Partners
Hadden, David	Ove Arup and Partners
Beairsto, Michael	Ove Arup and Partners, P.C.
Melendez, Enrique	Paragon Project Resources
Seid, Alex	Parsons
Massey, Sara	Passero Associates, LLC
Carter, Jim	Piedmont Triad Airport
Olivier, Jeanne	Port Authority of NY and NJ
Reis-Filho, Jorge	Port Authority of NY and NJ
Chambers, Charles	Priva Technologies
Muller, Peter	PRT Consulting
Smallback, Robert R C	Smallback Consulting
Campbell, Henry	Raleigh Durham Airport
Connolly, Liam	RAA
McGhee, David	Ross & Baruzzini
Robie, Michael H.	Ross & Baruzzini
Barry, Ann	Ross & Baruzzini, Inc
Hankins, Bonnie	Sacramento County Airport
Pilgrim, Michael	SAIC
Welch, Clint	San Diego County Airport
Dickie, Kim	San Francisco Intl Airport
Foster, Paul	San Francisco Intl Airport
Mattingly, Bob	Sarasota Bradenton Intl Apt
McCosby, Fred	Savannah Airport
Samlaska, Christian	Sea-Tac Intl Airport
Underhill, Emily	SW Florida Intl Airport
Condon, Tom	Sys. Development Integration
Zoufal, Donald R.	Sys. Development Integration
Clow, Michael	Tallahassee Regional Airport
Pollard, David	Tallahassee Regional Airport
Pak, Han	The JW Group Inc.
Willis, James	The JW Group Inc.
Bender, Gloria	Trans Solutions
Miller, Eric	Trans Solutions
Hill Ward, Nancy	TranSecure Inc.
Kosatka, Art	TranSecure Inc.
McGuire, James	TranSecure Intl, Inc.
Tucker, Courtney	TranSecure Inc.
Glasgow, Karin	TSA TSNM
Mahfouz, Stafford	Tyco International
Steele, Anne	U.S. Customs/Border Protect.
Terry, Staci	U.S. Customs/Border Protect.
Creech, George	U.S. DHS
Fawsett, Bradley	U.S. DHS
Schultz, Harry	U.S. DHS/TSA
Thomas, David	U.S. DHS/TSA
Zolghadr, Morvarid	U.S. DHS/TSA
Chaves, Jose	U.S. DHS/TSA, Airports
Cammaroto, Bob	U.S. DHS/TSA OST
Prediger, Susan	U.S. DHS/TSA—Sec. Tech.
Coeur, Ian	U.S. DHS/TSA TSNM
Di Rocco, Marie	U.S. DHS/TSA TSNM
Duffy, Michael	U.S. DHS/TSA TSNM
Jenkins, Annmarie	U.S. DHS/TSA TSNM
Lucini, Dawn	U.S. DHS/TSA TSNM
Prokop, Jim	U.S. DHS/TSA TSNM
Runde, Chris	U.S. DHS/TSA TSNM
Brecht-Clark, Jan	U.S. DOT Research & Tech.
Blumenthal, Don	University of Michigan
Anthony, Thomas	University of So. California
Swinehart, Steve	URS Corp
Adams, Mark	URSCorp
Lind, Archie	URSCorp
Johnson, Glenn	Victims of Pan Am 103
Connor, Michael	Wilkes-Barre/Scranton Apt
Kolman, Heath	XIP Consulting

TABLE OF CONTENTS

FIGURES

TABLES

PART I
OVERVIEW

Section A—Introduction

Airport security planning and design can sometimes seem a bit confusing; there are many fundamentally different elements to be considered, all of which must be integrated to work smoothly together as the threat continues to change and the airport's physical, electronic and regulatory security environment must constantly adjust. There are currently very few new airports and relatively few new terminals being built. The majority of changing security requirements will be accomplished in existing facilities that are often 15-20-25 years old and not designed to accommodate today's security measures and technologies. This publication is intended to bring an airport-wide focus to the various planning and design issues surrounding airside, landside, terminal, perimeter, IT, surveillance, access control, and indeed, to the unsecured but critical publicly accessible side of the airport. This guidance contains no legal or regulatory mandates. The planning and design concepts are current as of the 2011 publication date and will likely be updated as regulations and technologies change.

The document consolidates information developed through the participation of the Transportation Security Administration (TSA) and other government and aviation industry and airport professionals. The information contained herein was gained through the experiences of represents a broad range of aviation security programs and projects at numerous United States 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 presented in this document is the fourth update since the series was initiated by FAA, adopted by TSA, and is revised and updated periodically as lessons are learned, and regulations, security requirements, and technologies change. In particular, the modifications found in this iteration are most extensive in the chapters regarding baggage screening systems, passenger screening checkpoints, and access control systems, including biometrics, all of which have experienced very significant changes in recent years. There is also new material addressing command and control facilities and concept of operations (ConOps) due to the growing complexity of airport security systems.

In response to the September 11, 2001, terrorist attacks in the United States, and with the potential for future attacks, the President signed into law the Aviation and Transportation Security Act (ATSA), 115 Stat. 597 on Nov. 19, 2001.

The creation of the Dept of Homeland Security (DHS) by the Homeland Security Act of 2002 (Public Law 107-296) realigned a patchwork of government activities into a single department with the primary mission to protect our homeland, resulting in a Strategic Plan for the most significant transformation of the U.S. government since WW-II.

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

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 common when forced to retrofit. Inclusion of airport security expertise early in the planning process will result in a better-coordinated and more cost effective approach to security.

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

Section B—Applicability

These recommended guidelines are provided for consideration by airport operators, airport planners and consultants, designers, architects, and engineers engaged in renovations and new airport facility planning, design or construction projects. Some of the recommendations 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; there is an entire appendix on that subject.

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 unfamiliar to the designer/architect. The authors consider it vital to understand the complexities of such processes and the range of alternatives available to the airport operator—and thus to the designer—before a design can appropriately accommodate space allocation, queuing, equipment, surveillance, power, and communications requirements, and other security infrastructure 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. It is not intended to suggest mandatory measures for any U.S. 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 49 CFR 1542) some suggestions may be useful for consideration by general aviation (GA) airport operators as well.

GA airport operators may also refer to a document developed by a joint TSA-industry working group in 2004, titled *Security Guidelines for General Aviation Airports,* currently available on the TSA Web site and expected to be updated in the near future.

Section C—Purpose

The purpose of this document is to provide guidance for professionals responsible for, and affected by, the planning design and integration of security into 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" in each chapter 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 operationally 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), Secured Area, and Sterile Area, which are defined in 49 CFR 1540 and 1542;
2. Flow of both passengers and employees from landside to airside and back;
3. Efficient and effective security screening of persons and property into Sterile Areas as described in 49 CFR 1542, including consideration for queuing space during peak loads;
4. Separation of security areas and/or use of required and recommended signage;
5. Identification and protection of vulnerable areas and assets;
6. Protection of aircraft, people, and property;

7. Blast mitigation measures;
8. Space and infrastructure for checked baggage Explosives Detection Systems (EDS) and devices;
9. Space for advanced technologies at passenger screening checkpoints;
10. Accommodation of integrated infrastructure for advanced surveillance, access controls with biometrics; and
11. Command and control capabilities for improved situational and domain awareness.

These guidelines also identify airport areas requiring special attention in the planning process, and are intended to result in systems that will not hamper operations, cause undue economic burdens, or turn airports into "armed fortresses." At the same time, the guidelines must not be interpreted to mandate specific requirements to be met by any airport. They may suggest numerous alternate 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 unique local needs and operational environment in a responsive and cost-effective manner.

Users of these guidelines are reminded that the installation of physical security, access control, screening, and detection equipment, and structures (and barriers, access control, screening, and detection equipment) are 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 and building code officials, emergency response agencies, operations and maintenance personnel, and other end-users and tenants should occur for effective and efficient airport security.

This document is designed to be used primarily in digital/electronic PDF format, although it is also easily used by hard- copy readers. In the electronic PDF version, listings in the Table of Contents, or any other link in the body of the text, are dynamically linked; simply click on the title heading or link and you will be taken to that section of the document. To return to your original place in the document, click the Adobe Reader's "previous view" button.

Within the body of text throughout the document, you will find hyperlinked text referring the reader to other related sections, topics and graphics within the document. For example, where unique terminology is not being clearly defined when used in the text for the first time, or where reference to a more complete definition is deemed useful, a hyperlink is provided to that term's location within Appendix G—Glossary. Similarly, there are extensive active links to relevant external resources and Internet Web sites such as regulatory references, government and industry publications and reports, and technical standards, to name just a few. These links will keep the reader within this document, going to the complete list in the bibliography, which links can in turn be followed to the outside Internet source at the reader's convenience.

Section D—Background

The Aviation Security Improvement Act of 1990 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 of the President's Commission on Aviation Security and Terrorism, and recognized that 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 law: 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.

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, 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, to include the affected aircraft operators and tenants, fire code officials, building code officials, and local FAA and TSA officials, local emergency response personnel, and 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 and the sometimes- overlapping areas of control and managerial jurisdiction spelled out in each airport's site-specific 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 U.S. airports are addressed in the CBP Airport Technical Design Standards For Passenger Processing Facilities and in separate FWS and PHS standards. These contain the physical characteristics of the FIS area and set requirements for the design of new or remodeled airport terminal building facilities for CBP processing of international passengers and their luggage arriving in the United States.

The CBP Airport Technical Design Standards discuss passenger and baggage flow and terminal building space utilization including space requirements 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 early 2011, the CBP Design Standards were being updated by CBP to include Unified Passenger Processing, Preclearance Facilities, General Aviation Facilities, and other facility requirements.

The reader should refer to the most current CBP standards when accommodating those agencies' requirements in an airport design.

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

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

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

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

Section I-B—Applicability Checklist:

□ **Airport Facilities**
- 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
- Security Assessment

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

Section I-C—Purpose Checklist:

□ **Identify Key Concerns in order to:**
- Restrict access to security areas
- Control the flow of people
- Provide efficient security screening
- Protect vulnerable areas & assets
- Protect aircraft, people & property
- Address blast mitigation measures
- Provide space for EDS & ETD devices
- Provide space for EOD operations
- Airport Law Enforcement

□ **Identify Early Coordination needs with:**
- 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**

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

THIS PAGE INTENTIONALLY LEFT BLANK

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. Ensuring 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 are directly involved with the airport operator and should be consulted during all phases of any project.

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

Planning for security should be an integral part of any design project undertaken at an airport. The most efficient and cost-effective method of instituting security measures in 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 for the protection of the general public, the facility, passengers, and airport and air carrier personnel can result in costly modifications and delays.

Approaches to physical security should be based on applicable Federal, State, and local laws, regulations, and policies to ensure the protection of all persons and assets (including information systems and data). At a minimum, a physical security approach should include:

1. A vulnerability assessment, including a check of regulatory compliance (refer to Appendix A) to evaluate the existing security at an operational airport or a comprehensive security plan evaluating the potential vulnerabilities at a new facility or site;

2. A Concept of Operations (ConOps) that considers the physical and operational needs of all users and outlines the proposed approaches to planning, design, and integration to meet those requirements. The ConOps, properly developed, is the pre-cursor to all that follows, setting the stage for the coordination and integration of all new or upgraded safety and security systems and functionalities. ConOps is discussed in greater detail in Appendix E, Command and Control.

3. Periodic inspections to ascertain whether a security program and its implementation meet pertinent Federal, State, and local standards or regulations;

4. A comprehensive and continuing security and threat awareness and education effort to gain the interest, support and participation of employees, contractors, consultants, and visitors; and

5. Implementation of procedures for taking immediate, positive, and orderly action to safeguard life and assets during an emergency. This will typically be accomplished primarily through the 14 CFR § 139.325 FAA-required Airport Emergency Plan (AEP), coordinated with airport security contingency measures.

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, aviation security risk assessment is composed of the results of threat analysis, vulnerability assessments, the assets to be protected, and the resulting consequences. Airport security should reflect the risk status and financial resources of each specific airport. More than 90 percent of the air carrier airports in the United States 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 as they strive for effectiveness.

Section B—Facility Protection

The airport operator has a responsibility to provide a safe and secure 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 dangerous substances. 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. Some more advanced technologies can reach outside the fence to identify approaching threats, or may be used in an environment where there is no fence or physical barrier, such as a water boundary or swamp.

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

Section C—Planning Facility Protection

The objective of facility protection planning 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 airport operations should be considered when planning for the protection of an airport facility. *Figure II-C-1* 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 that are more comprehensively shown on an FAA-approved Airport Layout Plan (ALP). The ALP is one of the first documents suggested for review that will show the airport property and the facilities at a particular airport.

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

   b. Security Areas Basic Requirements (*Table II-C-1*) provides general comparative descriptions and regulatory requirements (including training, criminal history records checks (CHRC), and ID display) for the three basic airport security areas: Secured Area, Security Identification Display Area (SIDA), and Air Operations Area (AOA), defined in 14 CFR 153.3. 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.

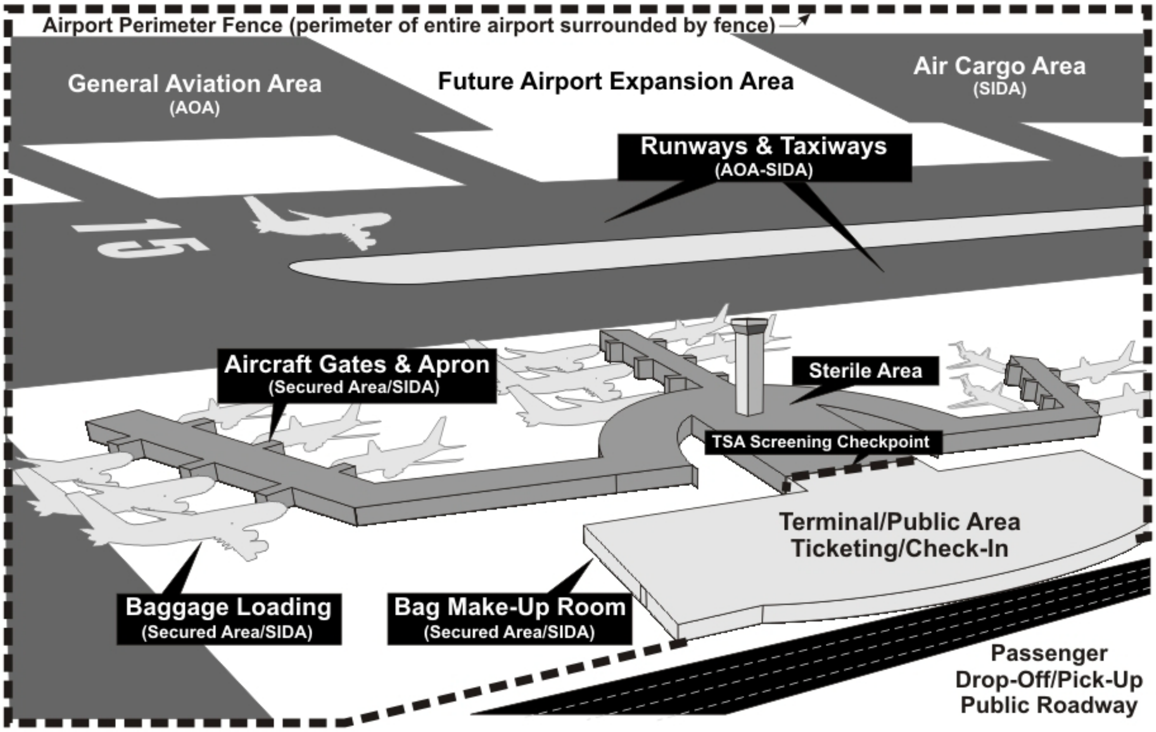


Figure II-C-1—Security Areas General Depiction

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 strong security and ease of movement for both passengers and employees. Refer to 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. Domestic and international threats and the general integrity of the U.S. transportation system

d. Facility location, size, and configuration;

e. Extent of exterior lighting;

f. Presence of physical barriers;

	Secured Area	**SIDA**	**AOA**	**Sterile Area**
Regulatory Requirements	1. Access controls meeting 49 CFR 1542.207. 2. Security training 3. Full CHRC and TSA Security Threat Assessment (STA) 4. ID display/challenge	1. No access controls required by regs. 2. Security training 3. Full CHRC and TSA Security Threat Assessment (STA) 4. ID display/challenge	1. Basic access controls meeting 49 CFR 1542. 2. Provide security information 3. STA required	1. Access controls meeting §1542 or screening per §1544. 2. Controls per Airport Security Program 3. CHRC and STA required
Security Level	Highest level of security including access controls, training, CHRC, STA, and ID display/challenge procedures.	SIDA relates to ID display and CHRC/STA only. Access controls are determined by requirements of AOA, Sterile, or Secured Area location	Broadest application of security; requirements are not specifically set forth in §1542. STA required	Sterile area(s) may be SIDA depending upon the Airport Security Program. CHRC and STA required
Relational Description	A Secured Area is always a SIDA, because all three SIDA elements are present: Training, CHRC/STA, and ID display/challenge procedures. However, the Secured Area goes beyond SIDA by also requiring access controls.	SIDA lacks access controls, so a SIDA cannot be a Secured Area.	The AOA requires only basic access controls, but sets no specific standards beyond those adopted locally in the airport security program	The Sterile Area begins immediately after the screening checkpoint(s) and extends to the boundaries of the Secured Area and/or SIDA, where access controls are required to enter the more secure areas.

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

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, and intermodal transportation facilities.

4. Physical Protection

Airport and aircraft operators provide 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.

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, airport operators also need to keep records of incidents, personnel access, or other activities. Some of the records (such as personnel access) may be maintained automatically. 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 operator 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 operators 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 in many instances these are simply promises to give aid, not delegations of authority, and are sometimes conditioned on whether the other jurisdictions may have their own simultaneous emergencies underway.

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, as similar mitigation measures may apply to a greater range of natural disasters.

Section II-A—General Checklist:

□ **Advance Planning**

□ **Determine User Requirements in the Concept of Operations**

□ **Physical Security Program**

- Vulnerability assessment
- Periodic inspections
- Continuing security education
- Emergency procedures

□ **Consult with Experts in Aviation**

□ **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

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 ensure 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 area of an airport usually 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, access to which is controlled. ICAO (International Civil Aviation Organization), in Annex 17 to its founding convention covering security states it more simply: "the movement area of an airport, adjacent terrain and buildings or portions thereof, access to which is controlled."

Typically, the airside is beyond the security screening stations and restricting perimeters (fencing, walls or other boundaries) and includes runways, taxiways, aprons, aircraft parking, and staging areas and most facilities 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 Air Operations Area (AOA), Security Identification Display Area (SIDA) and Secured Areas, the airside must be entirely nonpublic. Further information on these security requirements is contained in Security Areas.

The choice as to where the airside perimeter fencing or barrier may be located often depends on the surrounding environment and access roads, and may be one of the most critical decisions in designing or renovating an airport. In addition to the factors discussed in Facilities, Areas and Geographical Placement consideration of the following factors is essential in 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 airport operator must be able to maintain required airside operational clear areas and have adequate emergency response routes to allow first responders to meet appropriate response times.

b. Landside

Landside infrastructure is separate from terminal and airside facilities. In general, the landside facilities include patron and other public parking areas, walkways, public access roadways, rental car facilities, taxi and ground transportation staging areas, and any on-airport hotel facilities.

Landside facilities provide both traveling passengers and the non-traveling public with access to the terminal and airside of the airport. Since the landside includes all non-airside areas (other than the terminal(s) or airside), 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.

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

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

c. Terminal

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

When considering passenger and baggage screening security provisions, it is important for planners and designers to distinguish the commercial terminal from the general aviation terminal where charter and private passenger activity typically occur. It is also important to note, however, 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 often 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 of a terminal 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) or Vehicle Borne Improvised Explosive Device (VBIED) is highly beneficial when addressing blast protection measures. A centralized terminal can also minimize the communications interference that might be caused by adjacent, non-airport facilities.

2. Security Related Areas

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

a. Air Operations Area (AOA)

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

The airport operator is required to control and prevent access to the AOA, control movement within the AOA, and control unauthorized penetrations of the AOA. TSA regulations do not specify how to accomplish this requirement but rather leave 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. The AOA is a major portion of the area within the fence or other barrier that defines the airside/landside boundary of the airport. Exceptions to this may occur when electronic barriers or natural barriers, such as rivers and coastal waterfront, are being used to delineate boundaries. However, when considering whether any natural barrier is an appropriate boundary, the airport operator should consider the findings of the airport risk assessment or vulnerability assessment and whether the natural barrier should be complemented with other types of boundary protection. Special attention should be given to areas near the airport boundary where large bodies of water are used as public recreational or fishing areas near the airport boundary. The AOA is required to have a distinct, securable boundary line. Refer to Boundaries for more information and to Part II Section C—Planning Facility Protection, and Appendix A, Airport Vulnerability Assessment Process.

When allocating AOA space, consider that the AOA requires fewer specific security measures than the higher requirements of SIDAs or secured areas. Therefore maintenance or construction staging areas can have simpler access outside the more critical areas, and perhaps reduce the amount of man- hours needed for identification media issuance and revalidation, background checks, and security training. Further discussion is found in Facilities, Areas and Geographical Placement.

b. 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, which have a security program under 49 CFR 1544 or 1546, enplane and deplane passengers and sort and load baggage. It includes any adjacent areas that are not separated by adequate security measures.

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

Although the secured area generally includes portions of the landside and terminal, it is desirable to locate secured areas contiguously or as close together as possible to maximize ease of access by response personnel, utilize common areas of closed circuit television (CCTV) surveillance coverage, and minimize requirements for redundant boundaries and electronic access controls. Where there are several unconnected secured areas, such as baggage makeup areas, movement areas, safety areas, etc., each may require separate but integrated electronic controls.

c. 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, and specifically it is an area requiring display of an authorized identification media.

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

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

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

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

e. Exclusive Use Area

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

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

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

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. ATSPs are similar to exclusive use areas, except that tenants are not regulated parties.

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

Where tenants other than air carriers elect to undertake under their own security programs under 49 CFR 1542, such areas should be limited to the tenants’ immediate boundaries and sphere of influence, and should accommodate security requirements for contiguous boundaries with other tenants and/or the airport and airlines.

3. Assessment of Vulnerable Areas

a. Basic concepts of security risk management dictate that the security system provide the appropriate level of security for all of the assets to be protected, determined by an assessment of the perceived threat to those assets. At the facility planning stage, it is prudent to consider the relative "value" (or consequence of loss) and economic impact of all assets. There are many high value assets at an airport to consider, such as: aircraft (with or without passengers aboard); air traffic support facilities (tower, radar, weather, communications); terminal building(s), groups of the public or employees; fuel storage; critical infrastructure (power, water, communications) and surface vehicle access 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 (the described AOA, Secured Areas, SIDA, etc.). Since barriers and controls differentiate and limit access to these areas, this can lead to the assumption that anyone or anything found in the area is authorized to be there. This suggests a common vulnerability: Once inside the controlled area, an intruder may move about with relative ease, without encountering additional controls. For example, if an intruder breaches the fence line (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 misuse of emergency exits 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.

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).

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. Innovative designs that satisfy both passenger convenience and separation distance for blast mitigation should be sought, including potential facility design to minimize large congregations of people close to points of vehicle access or drop-off, or blast resistant walls and barriers.

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

g. A potential vulnerability also exists in 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, can 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 may 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. Infrastructure provisions for screening equipment at these locations would enable future inspection capability with significantly less impact. The same locations may also be considered as sites for inspection of deliveries of commercial goods, or for the future possibility of security requirements being 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 GA, commercial and industrial buildings, etc., which, while not necessarily recognized as the main target of terrorist activity, might still be in the path of such an attack. Or at the very least, these areas might be subjected to common crime, e.g., 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 operator, but it is important to look at the entire airport environment, make those determinations, and bring every affected entity into the early planning discussions, if for no other reason than to establish early on where the lines of responsibility lie. The airport operator must also keep careful records of these determinations and consider putting those agreements and lines of demarcation in writing, possibly as conditions of the lease, or into exclusive area or ATSP agreements.

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 automated 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 power for priority provisions (i.e., lighting, communications, etc.).

4) HVAC systems have important functions during extreme weather conditions because they control and maintain ambient temperatures for equipment, and thousands of passengers and employees. However, in doing so, HVAC equipment provides fresh air or heat circulation, which can become an attractive target or vector for attack. The security design should consider placing fresh air intakes in nonpublic areas whenever possible to control access to such intakes. If it’s not feasible to locate the air intakes in nonpublic areas, the security design should consider providing a capability to monitor publicly accessible air intakes (e.g., use of video cameras). Additionally, the security design should also provide for the capability to isolate sections of the building, and to vent sections of the building by using a positive air pressure. See Appendix B Airport Chem-Bio Protection and Response for more on design to prevent or mitigate chem-bio events.

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

6) Fuel supplies for vehicle and aircraft operations 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 for firefighting, and human emergency support, etc. 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, or the possibility of an alternative source.

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 are "critical assets" and should be secured by access control and CCTV systems. When network cabling traverses public areas, metal conduit should be used to protect the cabling.

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 also support airport operations. Dependence on carrier cellular services should be minimized as these networks are often saturated by traffic during emergencies. A standards-based wireless extension of the airport local area network (LAN) can be valuable in emergencies provided that operating frequencies and access point coverage have been properly designed and coordinated with all users including tenants.

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

It is important to note that all of the Seismic Laws and 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, as an aid to the designer, TSA recommends that the following sources of information be reviewed to determine the requirements.

1) Public Laws 95-124 and 101-614, "The Earthquake Hazards Reduction Act of 1977 as Amended."

2) Executive Order 12699 of January 5, 1990, "Seismic Safety of Federal and Federally Assisted or Regulated New Building Construction."

3) Executive Order 12941 of December 1, 1994, "Seismic Safety of Existing Federally Owned or Leased Buildings."

4) ICBO (International Conference of Building Officials (ICBO), "Uniform Building Code (UBC)," 1994, and amendments to include the 1994 National Fire Protection Association (NFPA) 13 Standard for Building Fire Sprinkler Systems.

5) BOCA (Building Officials Code Authority (BOCA), "National Building Code."

6) SBCCI (Southern Building Code Congress International "Standard Building Code."

7) 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.

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

4. Chemical and Biological Agents

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

Some measures that should be considered to help mitigate a potential chemical/biological attack include:

a. 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.

b. 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.

c. 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.

d. 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 with openings facing away from public exposure.

e. Coordinate the smoke control system and emergency power with the chemical/biological alarms and ventilation system.

f. 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 Counterterrorism) program, the Sandia National Laboratories issued "Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism," co-authored with the Lawrence Berkeley National laboratories.

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 (e.g., bodies of water) in the planning and design process. However, when considering whether any natural barrier is an appropriate boundary, the airport operator should take into account the findings of the risk and vulnerability assessments prepared for the airport and whether the natural barrier should be complemented with other types of boundary protection. Again, special attention should be given to areas where significant bodies of water are used as public recreational or fishing areas near the airport boundary. Access points for personnel and vehicles through the boundary lines, such as gates, doors, guard stations, and electronically controlled or monitored portals, should also be considered. There are additional 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, CCTV monitoring systems, and signage.

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

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

Various boundary/barrier and access point types as well as security measures 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 the sensors and response to intrusion alarms. *Table III-A-1* shows some of the available types of fence fabrics with American Iron and Steel Institute (AISI) and American Society for Testing and Materials (ASTM) ratings.

Chain link fencing is the most common type of fencing and is often the most cost-effective solution when deterrence, as opposed to the prevention of forced entry, is the primary security objective. Chain link fences are often constructed with seven (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. Fabrics should be secured to the fence posts and to the bottom rail in a manner that makes it difficult to loosen the fabric. Fences configured in this manner are shown in *Figure III-A-1.*

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, the fence line should be located inside the airport property line to prevent encroachment on adjacent property by the angled barbed wire topping or its outriggers.

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

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 and run-up areas. A taut fence fabric is often required under such circumstances.

The 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.

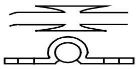
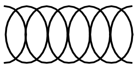
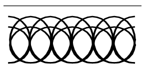
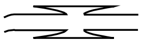
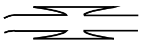
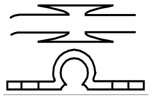
	PRODUCT	APPLICATION	SIZES	WT / ROLL	MATERIAL	ATTACHMENT SPACING LENGTH	BREAK LOAD
	RAZOR RIBBON—Single coil with core wire	Medium security fence topping	18" 24" 30"	13 lbs. 17 lbs. 21 lbs.	AISI 430 Stainless steel .098 dia. high Tensile wire	6"—16.6'7 9"—2'5 18"—5'0	2800 lbs.
	RAZOR RIBBON—single coil with wire concertina style	Ground barrier Max. security fence topping	24" 30" 36"	15 lbs. 19 lbs. 23 lbs.	AISI 430 Stainless steel .098 dia. high Tensile wire	12"—1'5 16"—2'0	2800 lbs.
	RAZOR RIBBON MAZE—Concertina style, double coil	Ground barrier Max. security fence topping	24" inside 30" outside	34 lbs.	AISI 430 Stainless steel .098 dia. high Tensile wire	12"—1'5 16"—2'0	2800 lbs.
	MIL-B-52775 B Type II austenitic double coil	Ground barrier Max. security fence topping	24" inside 30" outside	35 lbs.	AISI 301/304 stainless steel .047 dia. stainless wire rope	24"—6'6	2250 lbs.
	MIL-B-52775 B Type IV austenitic double coil	Ground barrier Max. security fence topping	24" inside 30" outside	35 lbs.	AISI 316 Stainless steel .047 dia. stainless wire rope	12"—1'5 16"—2'0	2250 lbs.
	RAZOR RIBBON—single coil	Min. security fence topping. Commercial use.	18" 24"	9 lbs. 12 lbs.	AISI 430 Stainless steel	6"—16.6'7 9"—2'5 18"—5'0	1260 lbs.
	BAYONET BARB—Concertina	Ground barrier	27½" 37½"	23 lbs. 34 lbs.	ASTM A 526 Zinc galvanized .098 dia. high Tensile wire	20"—5'0	1300 lbs.

Table III-A-1—Fence Types and Fabric

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.

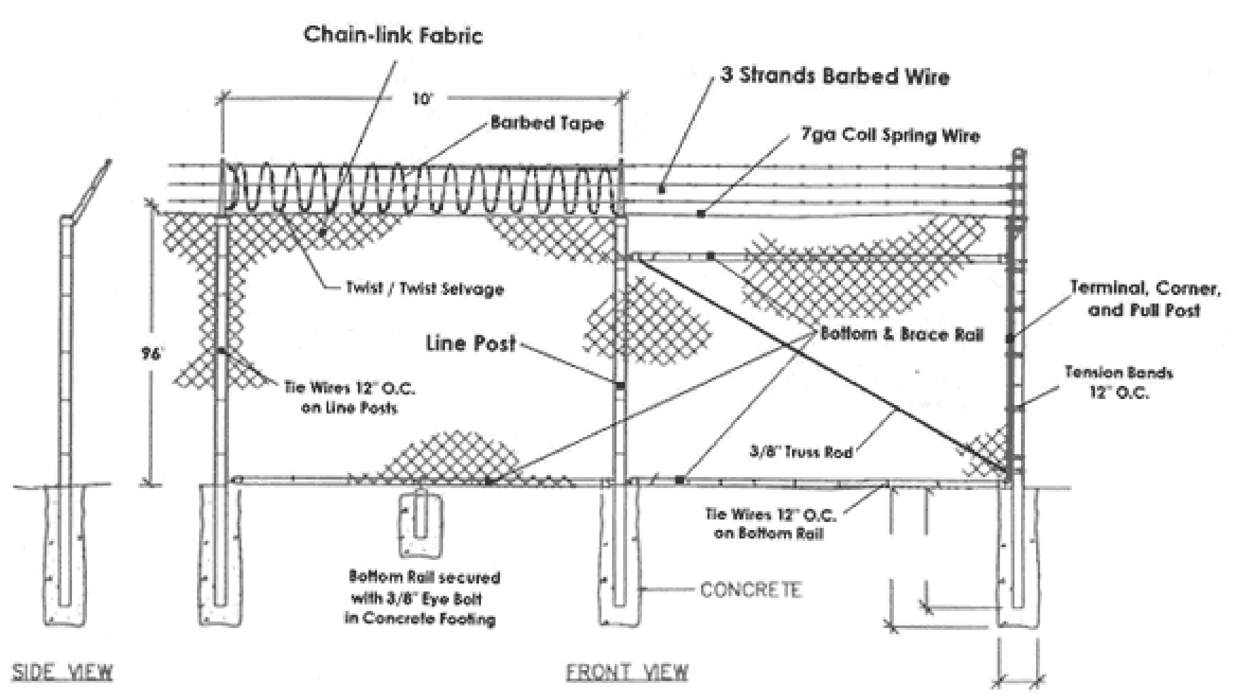


Figure III-A-1—Chain Link Fence Barbed Wire Configurations

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 for 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 depend on the nature of the business being conducted inside and the level of continuous access required by personnel. Building design should ensure that fire escapes or maintenance access ladders do not provide an unobstructed path from the public side to airside.

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 walls are less climbable than security fencing or other barriers that offer hand-holds.

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

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

b. Electronic Boundaries and New Technologies

In the case of boundaries that are monitored by electronic sensors, motion detectors, infrared or microwave sensors, etc., these are clearly intended to serve essentially the same security functions as other detectors but are simply employing other technologies, usually with somewhat higher maintenance costs. Usually 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."

While this document is focused on planning and design during the initial planning for current projects, new facilities such as terminals may sometimes take four or five years from the drawing board to processing the first aircraft and its passengers. When planning that terminal, and all other related facilities requiring a security perspective, one must also take into account continuing developments throughout the airport industry and the technologies that contribute to its secure well-being. While it may not be possible or even prudent to adopt first-generation beta-version technologies (although there may also be some corresponding advantages in such an approach), it is virtually certain that technology developments in many areas will afford new security capabilities and new requirements in the 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 personnel to monitor and respond to a wide range of alarms. This includes the use of automated system analyses and alerts, thereby expanding an operator's "vision" and capability several fold.

Whether this is a necessary, immediate, or even desirable course of action for your airport, as new technology becomes tested and available, it may 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. Planners can avoid the need for such costly actions as re-trenching, replacing limited panels, or relocating camera positions, etc.

One such technology is the adaptation of the existing FAA Airport Surface Detection Equipment (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-2*.

1) The TSA's Transportation Security Laboratory has successfully demonstrated the utilization of existing FAA ASDE radar to provide perimeter and airport surface surveillance at a category X airport under a pilot project initiative. The scope of the pilot project included the development, testing and implementation of a stand-alone prototype display processor system that received raw data from the

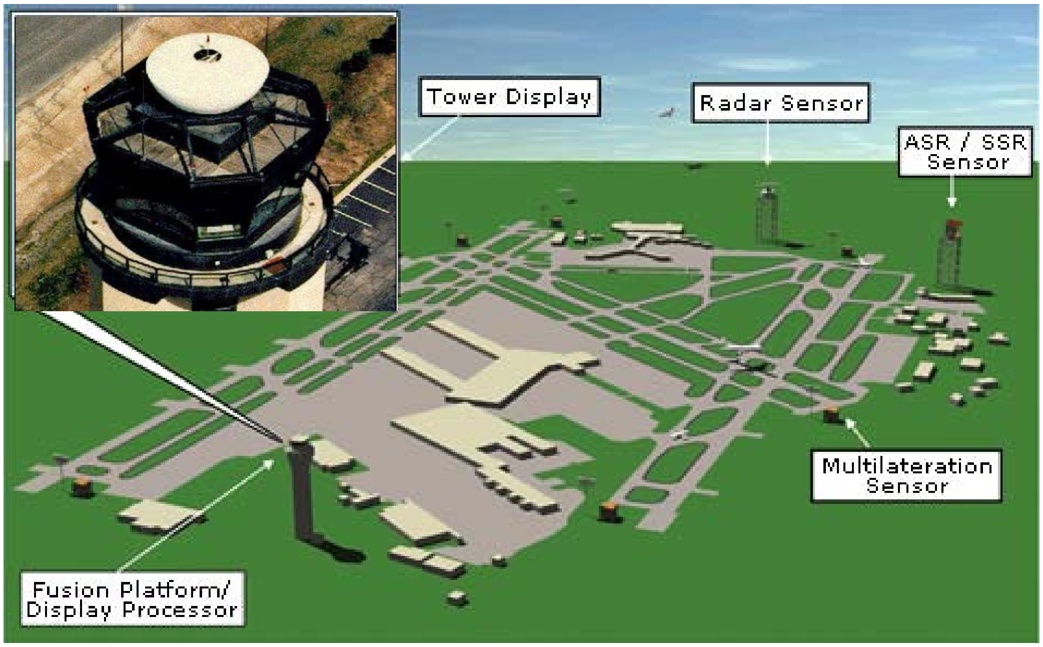


Figure III-A-2—ASDE Radar—Adaptation for Intrusion Detection

FAA ASDE radar, filtered out undesirable data, and utilized the real-time radar data stream for intrusion detection at the AOA perimeter. The system that was successfully tested provided the following capabilities:

- Intrusion detection along the AOA perimeter, including the segment of perimeter along a maritime waterfront;
- Automatic tracking of intruders on the AOA; and
- Delivery and display of alarm data to a workstation located at the security operations center.

2) To complement the intrusion detection system, the airport operator also installed CCTV cameras strategically located to provide for remote visual assessment of alarm conditions. Live and recorded CCTV images were displayed at the same workstation where intrusion alarms were displayed in the security operations center. The need for CCTV was identified during development of the project Concept of Operations (CONOPS)—refer to Appendix E Command and Control Depending on the specific requirements dictated by the airport operator, the intrusion detection system can be integrated into new or legacy CCTV systems.

3) Leveraging the existing ASDE radar for security surveillance could be a cost-effective enhancement to existing security measures for detecting intruders on the airport surface. Of course, the airport operator would need to provide the infrastructure and hardware required for system implementation, and make the legal and technical arrangements with the FAA in advance of project implementation.

c. Natural Barriers

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

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

Earthen material may also be used to create a visual barrier between any public road and the AOA. This can be accomplished through various methods such as trenching or the stockpiling of 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. 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 deterrent. This concept suggests that if an unauthorized entry were to occur at a particular location, the amount of time and the distance covered, combined with a high level of visibility, would significantly reduce the likelihood of the intruder reaching the critical area without detection and/or intervention. "Time and distance" may be considered as an enhancement to standard physical barriers/boundaries when those boundaries are relatively removed from the critical areas they are protecting.

Using the security design principle is known as "DDR," or, "Detect, Delay, Respond," in which protection of a relatively remote perimeter or facility. It 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 numerous intended access points through fencing or other barriers for both vehicles and pedestrians. Access points through buildings or walls are usually doors; guard stations or electronic means or controls may be also used. In all cases, the access point type and design may determine the effectiveness of the security boundary and control in that area. Hence, in all cases, the number of access points should be minimized and their use and conditions closely monitored.

1) Gates

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

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 generally high-throughput and should be designed for high-activity and long-life. These gates will take the most wear and tear and should be designed to minimize delays to users, particularly where piggybacking may be a concern. SIDA, secured area, AOA, and other security boundary gates that are high-throughput are the most likely candidates for automation and electronic access control.

b) Maintenance Operations

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

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

c) Emergency Operations

Emergency operations gates are used by on-airport and mutual aid emergency response vehicles responding to emergency situations, especially those involving an aircraft, 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.

The capability for emergency response vehicles to crash through frangible mounts at emergency operations gates should be considered during the gate design, as should alarms on those gates. Consider special paint markings to identify the frangible fence or gate sections to approaching response vehicles. However, the decision to provide such frangible mounts and associated paint markings should be carefully evaluated against the findings of the risk assessment or vulnerability assessment prepared for the airport. While such crash gates and markings would help first responders during emergency situations, there is always the possibility that perpetrators could also utilize these gates to gain unauthorized access to the facility.

Gates 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. Motor operator/controllers on gates should be located on the secure side of the gate. Battery / UPS backup power for the gate operator motor and for gate security devices (card readers, CCTV, buried induction loops, intercom, area security illumination/ lighting) to allow 2-hour gate open-close operation is essential to continuing vehicle traffic circulation during a power failure. In a sally-port gate, both the sally-port and vehicle gate would be similarly equipped with UPS

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 accommodate curb heights, wheel paths, potential obstructions, local weather/wind phenomena, and drainage issues throughout the full path of the gate and adjacent areas. Proper drainage grading, planned gaps in curbs, installation of concrete channels or mow strips below the gate path, and use of bollards to prevent obstructions within the gate path and protect gate equipment are all design considerations that may prolong the efficient operation of a slide gate.

If “tailgating” entry is a concern at 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 “sally port” or “vehicle entrapment gate”) is one method that could help prevent tailgate entry. Such gates are separated slightly more than one vehicle length apart and are sequenced so that the second gate does not open until the first has fully closed. Time-delayed closures are a viable alternative; sensor arrays can be used to monitor vehicle movement and assist in detection of tailgate entries. “Tailgating” and “reverse tailgating” (where a vehicle enters a gate 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 the unsecured public 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 card reader/pin pads, and recent advances in biometrics, to minimize labor costs and to be able to track personnel using specific doors to the AOA.

Unsupervised emergency exit doors providing egress from the terminal to the airside should be avoided if possible. If such doors are necessary, they should be equipped with audio and visual alarms. Consider mounting a police-blue lens (to differentiate security from fire alarms), preferably located on both sides of the door, which can be monitored from a supervised location such as an airport 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 operator should work with local fire and building code officials to determine the best systems allowable to accommodate both emergency and security needs. See also Public Emergency Exits for information regarding NFPA fire codes on emergency exits.

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

3) Guard Stations

Staffed guard stations to control access into a security area are appropriate at some locations. They provide a point of entry at which personal identification can be established and persons and vehicles can be permitted to enter according to local vehicle search program requirements.

a) Devices such as turnstiles, roll gates, pop-up barriers, or a remotely operated drop barrier gate may be used at guard stations to impede passage through the guard station until access authority is verified. In the case of vehicle access points, gates and barriers should provide the same or greater standard of security as any adjacent fencing to maintain the integrity of the area.

b) Tire shredders have also been used at vehicular access points in the past, although they are not a preferred option to providing protection against vehicular intrusion. While the tires on a vehicle can be shredded, there is no guarantee that the vehicle will be brought to a stop; it is possible to continue moving on shredded tires.

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

d) Sufficient space should be provided to direct a person or vehicle to one side for further inspection without blocking access for those following. Space should also be provided to allow vehicles refused entry to turn on the non-secure side and exit. Vehicle lanes and inspection stations should be provided in sufficient quantity to meet the expected traffic volumes, average inspection and processing times, and size of the largest vehicle entering the checkpoint. Stations may employ vehicle manifest pre-clearance checkpoints and special expedited clearance lanes for recognized deliveries. Dependable and instant communications from these stations to a central location must be installed, maintained, and frequently tested.

e) 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.

f) In some applications, a vehicle access point may be remotely controlled by use of a card reader or similar credential verification device, in conjunction with CCTV monitoring taking place in the 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 railings are useful. Consider protection of equipment from weather, including extreme heat or cold inside equipment enclosures, which can affect the operation of electronic and mechanical components. Heaters and/or fans are available as standard options for most access control devices, housings and operators.

b) Doors with Access Controls

There are numerous technologies available for controlling access through doors, 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 "legacy" systems the airport might wish to retain and integrate with new systems, and whether newer advances in technology might suggest a complete or partial replacement of the old systems to provide better security and security management. An extensive discussion of this issue is found in the RTCA document DO-230C, "Integrated Security System Standard for Airport Access Control."

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 sensor technology used (see Electronic Boundaries), these may be comparable in cost to mechanical ones.

The use of sensor line gates is typically feasible as a second, interior boundary where delays due to the mechanical operation of a physical gate are not practical, where space is limited, or where additional vehicle monitoring is desired. Sensor line gates are most often used to control vehicle access into a secured area or in cargo or maintenance areas where time is critical.

d) Automated Portals

Automated access portals are designed for high-throughput, performing access control in a high-speed, multi-user fashion, with a positive means of access denial of unauthorized persons and with the capability of preventing access if multiple or unauthorized persons attempt to enter. Where these are employed, the delay induced by door opening/closing is eliminated. These portals are designed to replace high-throughput doors where piggybacking is a concern or to add additional sensing technology to prevent explosives, drugs, or weapons from entering high-throughput areas.

Video analytics technology can monitor the direction of the intruder's movement, and automatically provide photographs of security violators, 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 locations.

5) Vehicle Inspection Stations, Blast Protection and Road Barriers

Staffed vehicle inspection stations and vehicle crash barriers in roadways may be necessary in high-threat areas to control access in and around the airport terminal and other airport facilities. Non-permanent measures may also be necessary during elevated threat levels or in high-risk areas. This aspect of airport design should begin with the results of the vulnerability assessment undertaken during the planning phase.

The purpose of vehicle inspection stations is to provide a location outside of the "blast envelope" in which to inspect vehicles that are approaching the airport terminal on the public roadway. Vehicle inspection stations may also be necessary at vehicle parking locations that are located within the blast envelope. Consider 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 bypass the vehicle inspection stations when necessary.

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 explosives-laden vehicles. There is a considerable body of knowledge on blast effects and protective measures available at U.S. government laboratories and agencies, under the auspices of the ASTM (American Society for Testing and Materials) under standard F2656-07 Standard Test Method for Vehicle Crash Testing of Perimeter Barriers.

Figure III-A-3 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. Consider complementary measures, such as physical setbacks of buildings and natural barriers or berms, when developing a blast protection solution. *Table III-A-3* displays the lethal blast radii for various types of threats and the types of blast-protection measures that might be considered to protect against each type of threat.

Previous Department of State performance requirements for vehicle crash barriers were based on the kinetic energy represented by the mass of a vehicle and its impact velocity. These “K” ratings are:

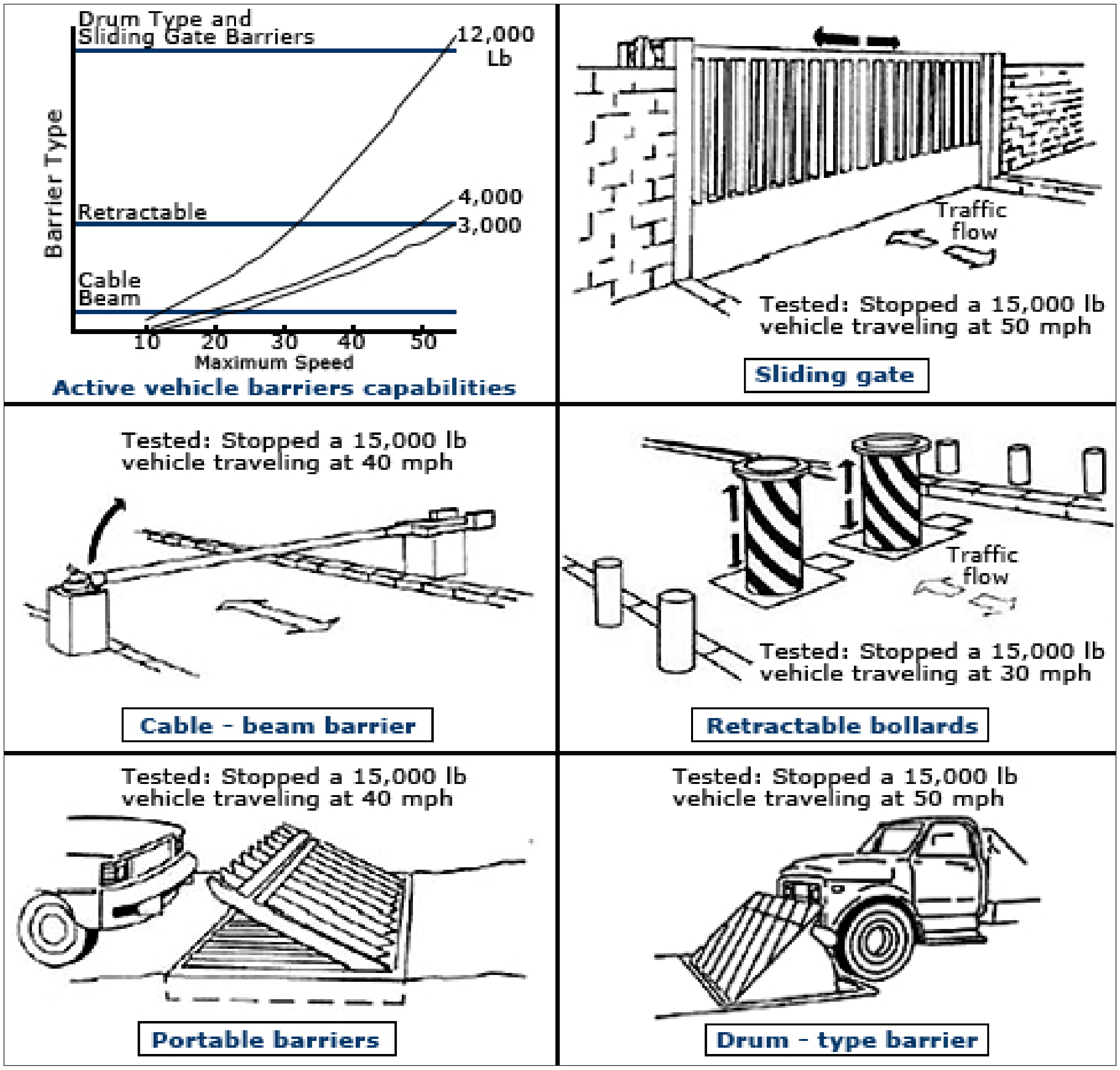
K4	15,000 lb vehicle impacting at 30 mph
K8	15,000 lb vehicle impacting at 40 mph
K12	15,000 lb vehicle impacting at 50 mph

To be certified with a Department of State (DoS) “K” rating, a barrier must have demonstrated the ability to stop a 15,000 vehicle and the bed of the vehicle must not penetrate the barrier by more than 36 inches. However, in early 2009, the State Department stopped the practice of issuing certification letters for perimeter barrier products. While the earlier certification letters remain valid, future testing and certification of perimeter barrier products is now carried out under the auspices of the ASTM (American Society for Testing and Materials (ASTM) under ASTM F2656-07 Standard Test Method for Vehicle Crash Testing of Perimeter Barriers. This ASTM standard provides a wider range of criteria (vehicle size/weight, vehicle speed, vehicle penetration), with four choices of vehicle weights (2,430 lb, 5,070 lb, 15,000 lb, and 65,000 lb) moving at speeds of 30 mph, 50 mph, and 60 mph. Additionally, the rating system takes into account vehicle penetrations ranging from “less than 1 meter” to “30 meters or greater.”

The earlier DoS ratings of K4, K8 and K12 can be described in terms of the ASTM rating system as being equivalent to the following:

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

In the above ASTM rates, “M” refers to the test vehicle weight of 15,000 lb, the “30,” “40,” and “50” refer to the nominal impact velocity of the vehicle, and “P1” refers to a penetration less than 1 meter.



Active vehicle barriers capabilities

Tested: Stopped a 15,000 lb vehicle traveling at 50 mph

Sliding gate

Tested: Stopped a 15,000 lb vehicle traveling at 40 mph

Cable - beam barrier

Tested: Stopped a 15,000 lb vehicle traveling at 30 mph

Retractable bollards

Tested: Stopped a 15,000 lb vehicle traveling at 40 mph

Portable barriers

Tested: Stopped a 15,000 lb vehicle traveling at 50 mph

Drum - type barrier

Figure III-A-3—Types of Road Barriers

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

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.

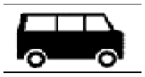
ATF	VEHICLE DESCRIPTION	MAXIMUM EXPLOSIVES CAPACITY	LETHAL AIR BLAST RANGE	MINIMUM EVACUATION DISTANCE	FALLING GLASS HAZARD
	COMPACT SEDAN	500 Pounds 227 Kilos (In Trunk)	100 Feet 30 Meters	1,500 Feet 457 Meters	1,250 Feet 381 Meters
	FULL SIZE SEDAN	1,000 Pounds 455 Kilos (In Trunk)	125 Feet 38 Meters	1,750 Feet 534 Meters	1,750 Feet 534 Meters
	PASSENGER VAN OR CARGO VAN	4,000 Pounds 1,818 Kilos	200 Feet 61 Meters	2,750 Feet 838 Meters	2,750 Feet 838 Meters
	SMALL BOX VAN (14 FT BOX)	10,000 Pounds 4,545 Kilos	300 Feet 91 Meters	3,750 Feet 1,143 Meters	3,750 Feet 1,143 Meters
	BOX VAN OR WATER/FUEL TRUCK	30,000 Pounds 13,636 Kilos	450 Feet 137 Meters	6,5000 Feet 1,982 Meters	6,500 Feet 1,982 Meters
	SEMI-TRAILER	60,000 Pounds 27,273 Kilos	600 Feet 183 Meters	7,000 Feet 2,134 Meters	7,000 Feet 2,134 Meters

Table III-A-2—Vehicle Bomb Explosion Hazard and Evacuation Distance Tables

[Department of the Treasury, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)]

d) It should be noted that security clear zones along perimeters or elsewhere, have no relationship with, and should not be confused with FAA-defined runway clear zones that have to do with aircraft approach slopes under FAR §151.9 and §77.27.

2) Security Lighting

Lighting of the area on both sides of gates and selected areas of fencing is highly recommended. Lighting can assure that fence/gate signage is readable, and that card readers, keypads, phones, intercoms, and/or other devices at the gate are visible and usable. Similarly, sufficient lighting is required for any area in which a CCTV camera is intended to monitor activity. Reduced lighting or sensor activated lighting may be considered for areas that have minimal traffic throughput in the off-peak hours. There is extensive discussion of lighting and camera issues in Section G of this book.

3) Locks

Advanced electronic lock and key technologies should be considered as well as the time-honored deadbolt lock, built-in door handle lock, or padlock and metallic key to secure a portal, particularly those portals that are low-risk, low throughput, or significantly distant from the main areas of concern or from communications nodes to the central control station. Note that securing perimeter access portals through the use of locks necessarily involves procedural elements such as a key management system, and the inherent difficulties of recording usage at numerous locations and reissuing all keys when some are lost or stolen. An important consideration in choosing lock systems is total life-cycle cost.

4) CCTV Coverage

a) 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 systems 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, with adequate CCTV surveillance to initiate detection and response.

b) Further information on CCTV Systems and coverage is contained in Section H, CCTV Surveillance and Video Detection Systems.

5) Signage

a) TSA requires signage on certain security boundaries and access points. Specific requirements are found in the ASP pursuant to 49 CFR 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 violation.

c) Many locations with access control or surveillance equipment 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 operator for policy, content, style and consistency. Based on local conditions, the use of multi-lingual security signage should also be considered.

e) Refer to the Terminal Section for additional airport signage information and to TSA checkpoint signage guidance available from TSA through the FSD.

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, or tampering with aircraft parts and equipment
- Non-reliance on large hangar doors/opening as a security boundary/demarcation line
- Location of loading/delivery docks landside

b. Aircraft Movement Areas

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

c. Aircraft Rescue and Fire Fighting (ARFF) Facilities

ARFF stations and equipment are a requirement of 14 CFR 139, Subpart D, Certification and Operations: Land Airports Serving Certain Air Carriers, which is administered by FAA. These facilities are clearly critical to an airport’s operations. 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).

The positioning of each ARFF station must consider emergency response times and routes should be considered when positioning each ARFF station. Thus, stations are located for minimum response times to required locations. ARFF vehicles may also 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. The administrative office area of an ARFF station may be open to public access, enabling persons having business with ARFF officers to enter these areas without access control. 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 operator staff to determine direction for the operational design.

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

The following are typical titles for locations from which airport operations are directed from during normal security operations, as well as during an emergency event. 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). A distinction is made between non- emergency (everyday operations) and emergency facilities, which are established for command and control operations during emergencies.

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

There are no hard and fast rules for these locations though most are in or attached to the main terminal. In all cases they should be located within a secured area. The designer should 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, or when multiple events are taking place. While ease of access to the airside is one primary consideration, there are numerous other concerns such as sufficient operating space for police and other support personnel, central location for access 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 and Airport Emergency Command Post under the Command and Control Appendix.

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. Most airport personnel offices are located in or near the terminal, and are secured (nonpublic) at least part of the time. Some airport offices, such as airfield maintenance or operations, are generally completely airside, but still behind access controls.

Most airport personnel offices are located in or near the terminal, and are secured (nonpublic) at least part of the time.

f. Belly Cargo Facility

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

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

The added flexibility in the location of a belly cargo facility, as well as the fact that it can be separate from the general cargo facility, enables a belly cargo facility to be designed with potentially higher security levels. Since belly cargo usually involves smaller quantities of public air cargo and U.S. mail, belly cargo facilities can be designed which have the potential for 100 percent 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 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 roadways.

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 coordinated by the airport planner and designer such that an interface takes place with FAA security requirements pursuant to FAA's ATCT design criteria. When the ATCT is in a remote airport location, it may require significant levels of protection as one of an airport's most critical operational facilities. Coordination between the FAA, TSA, and the airport operator is necessary in order to address all ATCT security needs and their impacts upon airport operations.

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 entire fuel farm and its above ground storage tanks, and should be access-controlled whenever possible to monitor all movements, including authorized traffic. Where distance precludes hard wiring to the main system, there are wireless technologies as well as freestanding electronic locking mechanisms available. CCTV monitoring, alarms, and sensing should be considered in and around fuel farms and storage tanks to alert law enforcement/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 are usually part of the airside/landside boundary; aircraft parking areas/ramps are located 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 document is available on the TSA Web.

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 and other interested parties is received.

k. Ground Service Equipment Maintenance (GSEM) Facility

Most airports maintain specialized areas for storage and maintenance of ground service equipment (baggage tugs, push-back vehicles, refueling trucks). These areas are often referred to as Ground Service Equipment Maintenance (GSEM) facilities and may also be used to service and maintain other airport and maintenance vehicles. As with other maintenance facilities, these areas may be landside or airside depending upon their needs and the amount and frequency of landside/airside transition.

Similar to other service and maintenance areas, particular attention should be paid to material and vehicle parking/storage areas, ensuring 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 reaching the terminal curbside areas. These areas are always landside as they involves public and private off-airport transportation services.

m. Hotels and On-Airport Accommodations

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

n. Industrial/Technology Parks

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

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 requirements, needs and choices may involve substantial amounts of coordination, both architecturally and procedurally. The results of determination of the security risk and vulnerability assessments involving catering operations should be evaluated in advance of design or construction of these facilities.

p. Intermodal Transportation Area

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

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 and is used for parking an aircraft when isolation is required due to security or other concerns. This location is subject to special security requirements as identified in the airport's ASP.

Detailed information is contained in Isolated Security Aircraft Parking Position within the Airside section.

r. Military Facilities

Some airports may have adjacent or on-airport military facilities, such as Reserve, National Guard, State, or U.S. 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 operator, FAA, TSA, and the government military facility should occur to consider both design and procedural accommodations. 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 ensure that the security and safety of such military facilities are not compromised by the placement of airport CCTV and access control equipment. See Unified Facilities Criteria UFC 4-010-02 for Department of Defense (DOD) Minimum Anti-Terrorism Standards for buildings used by the military.

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.

u. Passenger Aircraft Overnight Parking Areas

Passenger aircraft overnight parking areas are required to be airside and are usually adjacent to the passenger terminal, but may also be on a designated 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 1544.

Additional information is contained in Passenger Aircraft Overnight Parking Areas in the Airside chapter.

v. Rental Car and Vehicle Storage Facilities

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

See the Rental Car Storage Areas section 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 often isolated from other GA/FBO areas and require stricter, and more extensive, security measures. In many cases these areas will have their own, independent security/access control/CCTV system, as well as their own monitoring and security personnel. Still, procedural coordination and communication with the airport should occur.

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.

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 or access points to be landside. Special emphasis should be given to above-ground electrical substations.

z. "Through the Fence" Agreement

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

Where underground service ducts, storm drains, sewers, tunnels, air ducts, trash chutes, drainage structures, and other openings provide access to the airside or other restricted areas, security treatments such as bars, grates, 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.

<u>Section III-A-1—Airport Layout and Boundaries Checklist</u>:

- □ **Determine Requirements based on ConOps**
- □ **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

<u>Section III-A-2—Security Areas Checklist</u>:

- □ **AOA**
  - In general, AOA perimeter is defined by fences or natural boundaries
- □ **SIDA**
  - May be a separately designated area located on AOA
  - Not necessarily a secured area (access controls desirable, not required by regs.)
  - Smallest manageable contiguous size(s)
- □ **Secured Area**
  - Always a SIDA
  - 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

<u>Section III-A-3—Vulnerable Areas Checklist</u>:

- □ **Vulnerability Assessment (see Appen. 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:

□ **Determine requirements per ConOps**

□ **Physical Barriers:**

- Align with security area boundaries
- Fencing
  - Based on vulnerability, cost
  - Typical: 7' chain link + 1' barbed wire
  - Motion, tension sensing available
  - Ground clearance 4-6 inches
  - In critical areas, anchor bottom
- Interior walls—full height, floor-to-ceiling
- Exterior Walls—Minimize hand holds
- Electronic Boundaries
- Motion detectors, Infrared sensors
  - Stand-alone or with other barriers

□ **Natural Barriers**

- Bodies of water; trees, dense foliage

□ **Minimize Access Points**

- Plan for maintenance, emergency ops:,
- Delivery and maintenance vehicles
- Electronic Access Points
  - Automatic Gates, Induction loop
  - Bollards to reduce vehicle damage
- Access controls
  - RTCA DO-230C Integrated Standards

□ **Other Security Measures**

  - Clear zones, security lighting
  - Consider life cycle costs, not just initial capital cost
  - CCTV Coverage
  - TSA/FAA-required signage per Advisory Circular 150/5360-12C
  - Instructional/ legal signage; coordinate with airport policy

<u>Section III-A-6—Facilities, Areas and Geographical Placement Checklist</u>:

□ **Facility Placement Considerations:**

- Interaction among areas
- Types of activity in each area
- Flow of persons to/through areas
- Flow of delivery & maintenance traffic
- Need for security escorts

□ **Each Airport is Unique**

□ **Facilities:**

- Aircraft Maintenance Facilities
- Aircraft Overnight Parking Area
- ARFF Facilities
- SOC/CP
- Airport Personnel Offices
- Belly Cargo Facility
- Cargo Area
- FAA ATCT and Offices
- Fuel Area
- GA Areas
- GSEM Facility
- GTSA
- Hotels and other accommodations
- Industrial/Technology Parks
- In-Flight Catering Facility
- Intermodal Transportation Area
- Military Facilities
- Nav /Comm Equip
- Rental Car Facilities
- State/Government Aircraft Facilities
- Utilities and Related 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/operator or be delegated to a tenant or contractor operating on the airside or under a joint use agreement. Areas and functions which should be included in an airport's security program include:

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

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

a. Aircraft Movement Areas

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

First and foremost among the non-security requirements are the FAA safety and approach runway protection zone requirements, as described in 14 CFR 77. While the specific distance requirements vary by runway, taxiway and/or aircraft class and wingspan (See A/C 150/5300-13), they all share the same types of requirements noted below. Although these are not security related areas and may be made of various alternative materials, 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; and thrown objects, etc.; and visibility of the areas around the parked aircraft to monitor for unauthorized activity. Airport operators 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 be 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 (IAB) area, which is typically 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

The International Civil Aviation Organization (ICAO) Standards require the designation of an isolated security aircraft parking position suitable for parking aircraft known or believed to be the subject of unlawful interference, to remove and examine cargo, mail and stores removed from an aircraft during bomb threat conditions, or which for other reasons, need isolation from normal airport activities. This location is also referred to as a “Hijack/Bomb Threat Aircraft Location” or “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. (Additional guidance in ICAO Annex 14 (Aerodromes), Annex 17 (Safeguarding International Civil Aviation Against Acts of Unlawful Interference), and Doc 8973 (Security Manual).

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. 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, or aviation fuel storage tanks and pipelines, 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, by persons seeking to reach 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. 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. 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 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, should 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. 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.

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/Localizer Area
    - Approach Lighting System
- Passenger Aircraft Parking Areas
  - Safe distance to fence/public areas
  - Safe distance to parked aircraft
  - Safe distance—prevent vandalism
  - Monitor areas around parked aircraft 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
  - Separation of utilities and fuel
  - CCTV view -aircraft and area
  - Emergency staging area
  - Avoid public viewing/ areas

□ **Airside Roads**

- Restrict access to authorized vehicles
- Perimeter roads should be airside
- Perimeter roads 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

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

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

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

1. Natural Barriers

The use of natural barriers in the airport landside area may be advantageous in locations that cannot structurally support physical barriers or fencing, or where the use of fencing or physical barriers would cause conflict with aircraft navigation, communications, or runway clear areas beneath approach paths. As is the case in the airport airside area, with TSA approval, natural barriers may be incorporated into the security boundary of an airport in support of standard physical barriers or as a complement to additional security measures or procedures.

Refer to Natural Barriers for a description of possible natural barriers.

2. Landside Roads

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

When planning landside roads, bear in mind their proximity to security fencing and the potential for unauthorized airside access offered by elevated roadways and line-of-sight threats to adjacent areas of the terminal, apron, and/or nearby aircraft. When an alert is issued, consider potential methods and locations 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 include conduit and rough-ins at those locations for power, communications and security data lines. If physically possible, consideration should be given to the creation of a roadway system that separates cargo from passenger traffic.

a. Vehicle Inspection Stations

Staffed vehicle inspection stations to control access in and around the airport terminal during elevated threat levels are advisable to provide a location outside of the "blast envelope" in which to inspect vehicles approaching the airport terminal on the access roadway. In some instances, vehicle inspection stations are also suggested at vehicle parking locations if they are located within or adjacent to 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, to permit maximum visibility over the immediate area of the gate and to provide easy access for inspections. A sheltered checkpoint station could be a portable "plug-in" unit if utilities have been pre-positioned.

Sufficient space to direct a person or vehicle to one side for further inspection without blocking access for those following. Also, sufficient space for emergency vehicles and other preauthorized vehicles to by-pass the vehicle inspection stations.

Provide communications, including emergency and duress alarms, between any sheltered security checkpoint station and the airport security services office.

Ample vehicle queuing distance and inspection portals to avoid long traffic backups and delays during peak use times.

b. Roadway Design

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

Drop off and loading zones should be set as far away from the terminal as practical to minimize the blast effects of a vehicle bomb. 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 the inspection area. 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 area, rental car agencies, hotels, or remote parking with shuttle service.

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

3. Landside Parking

a. Terminal Patron Parking Design

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 effects from a vehicle bomb. Consider allowing temporary parking or inspections 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 directly in front of the terminal. Elevated security levels may require vehicle inspections.

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, first response, 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," devices that limit the height of vehicles that can park in a certain area by suspending an immobile steel bar at the limiting level, so smaller cars can 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, as well as turning radius accommodations for tow trucks for removal of suspicious or abandoned 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 need 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 24 hours a day, is no less important than that of parking areas for the traveling public, and should be treated similarly, especially where they are remotely located and/or 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. Space should also be allocated for employee screening checkpoints as appropriate. For cargo facilities, there should be no employee parking adjacent to cargo bay doors.

4. Landside Facilities

a. Ground Transportation Staging Area (GTSA)

GTSAs may present some unique 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.

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 should acknowledge the potential for persons to exit from the hotel on or near the airside, or to pass contraband from hotel windows to persons on the airside. While direct sight lines to active aircraft movement areas are often considered an attractive feature of airport hotel design, it is not a particularly desirable feature from the security point of view, considering potential trajectories from a close-in, publicly accessible, private hotel balcony. Other considerations include security design elements to accommodate the hotel cash-handling activities and vendor/supplier traffic at all hours of the day.

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. Both light rail and heavy rail systems are now being used to bring travelers to the airport, with automated people movers acting as circulators with a connection to a rail station, sometimes elevated with airside sight lines.

When planning, designing or renovating an airport, alternative modes for moving people in and out of an airport should be considered. When such intermodal alternatives are being discussed, security and safety concerns should 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 normally landside, and often are well removed from the terminal and possibly the airport itself. However, as these areas use not only security features such as fences and gates, but also access control and/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, then bollards, curbing or other structures should be planned to prevent vehicles from being parked in locations that would violate security clear zones. The requirement to maintain this security perimeter may also need to be incorporated into the respective tenant's lease agreement.

5. Access Control Portals (ACP)

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.

ACPs should be located away from the terminal and other critical infrastructure, such as ATC towers or radar systems, so that any means of attack will have minimal effect 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 use, maintenance operations, and emergencies.

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 are 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, as well as candidates for adversarial breach. Refer to the Access Control section of this document for further information.

b. Roads

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

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

6. Interior Spaces

When interior walls are used as security barriers, consider not only the wall type and construction material, but also the wall height. When possible, security walls should be full height, reaching not just suspended ceilings, but extend 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 are used to deter and delay the access of unauthorized persons onto non-public areas of airports. These are usually permanent barriers designed to be an obvious physical barrier as well as a visual deterrent, and can also serve to meet safety requirements.

1) Fencing

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

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

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

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

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

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

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

h) 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.

i) 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, and Standards for Specifying Construction of Airports. Refer also to Fencing section of this document for more information.

2) Buildings

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

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

Walls of solid materials should not have hand or foot holds that can be used for climbing, and tops of walls should have barbed wire or other deterrent materials. Jet blast walls are not necessarily good security fences, although appropriate design can aid in incorporating features of both, spreading the cost over more than one budget.

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

b. Lighting

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

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

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 in the secure airside when possible, maintenance contracts and service personnel identification media issuance and access may require utilities to be landside, although that must then also be secured. Special emphasis should be given to above ground electrical substations, and manhole access points outside the perimeter.

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

8. Systems and Equipment

a. Electronic Detection and Monitoring

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

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 normally subject to Federal airport security regulations, but during implementation of crisis contingency plans, they can be expected to be affected by special security measures. Prudent use of surveillance technologies such as CCTV and video analytics should be considered in monitoring areas of concern, in consultation with airport law enforcement, the airport security coordinator, 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 facilitate police/emergency response.

9. Emergency Response

a. Law Enforcement

Provide for a remote temporary police substation or presence in the vicinity of an incident.

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, mutual aid agreements, or unusual situations may require response by off-airport emergency or law enforcement personnel. In addition, some airport primary response personnel (such as for structural fires) may be from off-airport organizations, such as Explosives Ordnance Disposal (EOD) units or nearby community fire/EMT response. Both procedural and design-related coordination must occur, particularly where off-airport response personnel may need to enter security areas. Where special procedures or design elements may be required, 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 with access identification media.

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 appropriate 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 personnel and equipment.

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 desirable. This will allow for added coordination with less risk of secondary incidents and delays. This may be beneficial to off-airport emergency services requiring access through passenger checkpoints, response to major airport-related traffic incidents, on-airport structure fires or medical incidents, and on-airport emergency landings or crashes which could become off-airport traffic problems.

c. Life Safety Equipment

Consider incorporation of life safety (emergency medical) equipment, defibrillators and/or duress alarms in public and restroom areas and/or at locations where airport personnel deal directly with money, baggage, ticketing, and/or disgruntled persons. Emergency phones/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 TCUs will typically be stored within the terminal, it is important to determine how the responding bomb squad will gain access to the TCU, and how it will be transported throughout the terminal. Large

TCUs are designed to be hooked to the back of a vehicle and driven away. The TCU can be pushed by as few as four individuals; however slight inclines can be difficult 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/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
      - Minimize or distribute congested driver waiting areas
      - Sufficient night lighting
  - Hotels and On-Airport Accommodations
    - Possibly connected to terminal
    - Treated same as 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 area

Section D—Terminal

1. Terminal Security Architecture

From a security perspective, airport terminals are generally divided into two zones, usually known as "landside" and "airside." ICAO draws the line of demarcation at the screening checkpoint; from the U.S. point of view the airside typically includes secured areas, sterile areas, and the AOA. The security systems and procedures serve to transition the passenger from landside security concerns and measures to the airside, where security concerns and measures differ significantly: a transition from land based transportation systems to air based systems; a transition in the flow of passenger movement; and a transition in the management of airport operations.

This transitional aspect of airport terminal planning and design means the planners should accommodate some flexibility for various activities on both the landside and airside while permitting efficient and secure methods for operational transition between the two. The complexity of meeting the functional needs of the owners, operators, airlines, and users of an airport terminal requires a combination of transition strategies. Successful planning and design processes require the participation of the airport security committee (if one exists); 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 to develop appropriate collaborative strategies to meet current security requirements and provide the flexibility for future change. This chapter provides an overview of many of the concepts and methods involved in security planning and design of terminal building facilities. Other chapters throughout this document as well as links to a wide range of other resources provide considerable detailed guidance for security-related improvements in the airport environment.

a. Functional Areas

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

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

1) Approach roadways and parking facilities that have adequate standoff distances from the terminal;

2) Blast resistant façade and glazing materials or fabrications;

3) Surveillance systems (such as CCTV cameras, video analytics, microwave, etc.) at curbside, doorways and perimeters;

4) Structural columns and beams that are resistant to explosive blasts;

5) Vehicle barriers that prevent vehicle-borne IEDs from driving close or into the terminal; and

6) Capability for vehicle inspection stations with ample space for vehicle queuing and standoff distances.

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

b. Physical Boundaries

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

For further discussion on specific design aspects of boundaries and barriers such as walls and doors, see Airport Layout & Boundaries; Landside; Security Screening; ACAMS; and Video Surveillance.

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

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

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

c. Bomb/Blast Analysis Overview

Blast analysis and mitigation treatments are addressed at 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 by the airport operator.

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

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

1) When developing and evaluating blast resistant solutions, it is important to:

   a) Define the threat(s)

   b) Establish performance objective(s)

   c) 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 operator should choose the approach they believe is best for their respective facilities.

2) Priority should be given to implementing blast protection measures that:

   a) Are passive (and do not rely on personnel);

   b) Do not hinder airport operations and functions;

   c) Consist of durable materials (will not fade, discolor, or become brittle with time);

   d) Do not distract from terminal architecture and aesthetics; and

   e) Provide cost-effective improved blast protection.

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

   a) Structural—These are blast mitigation measures that can be employed to enhance the protection envelope around the terminal or reduce the need for vehicle inspections. Blast hardening the perimeter columns of the terminal is an example of this type of feature.

   b) Non-structural—These are blast resistant features that offer some measure of blast protection, but have no effect on the need to inspect vehicles or restrict parking during heightened threat levels. Installing blast resistant window treatments and strengthened and/or non-fragmenting trash containers are examples of this type of feature.

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

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

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

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 that may contain 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, 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 that such spaces are included in all search protocols. 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 "behind the curtain" activity must occur in support of passenger activities for the whole process to function smoothly. Much of the support activity occurs in areas and pathways that are out of public view and have no public access. Aircraft operator and airport personnel need access to various functions of the terminal on a continual basis, sometimes at a hectic pace. Concessionaires within the terminal should have a means of delivering supplies and materials to various locations without impacting passenger circulation. Airport system monitoring and maintenance functions need to occur away from passengers whenever possible.

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

Vertical circulation can be particularly problematic since building functions and levels of security are often stacked. Code-required exit stairs often double as service corridors requiring particular attention to security strategies along their length. Exit stairs should only egress to public areas. Uncontrolled exits to the aircraft operations areas (AOA) should be avoided. Elevators have very similar issues. Public elevators should not cross levels of security, although service elevators, by operational definition, typically access all levels, and may need access controls in some areas.

Airport police and other law enforcement entities often need secure nonpublic corridors. LEOs must escort persons to and 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

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

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

In some instances an automatic door in a security boundary might be considered, bearing in mind there are some safety and maintenance challenges. A large cross-sectional area may require an oversized entry such as a roll-up door. The operation of such an entry should be integrated with the security system so that security permission 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 usually considers contingencies for future growth and expansions of a terminal facility. Planning is done for expansions of public and support spaces, growth and distribution of airport systems, location or expansion of future security checkpoints and additional measures needed during periods of heightened security. Incorporation of additional space and utility terminations for expansion and contingencies both reduces cost for the later installation and execution of those measures and minimizes the operational impact when those measures are added, but may impact alternative interim uses for the space, such as concessions.

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

Because space is at a premium at an airport, areas designated for contingency use could also serve other purposes, such as public lounges, children's play areas, local artifact or commercial displays, etc., bearing in mind 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.

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 procedural responsibilities, such as at the screening checkpoint, which is a TSA responsibility, and for which TSA has some very specific design requirements, as do some other Federal stakeholders. For example, Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) have unique operating regulations, and each must address its security requirements early in the host airport's planning and design process. These functions will be considered in more detail throughout this document.

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

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

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

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 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 employees require full access to the entire terminal building and all related facilities. The access control chapter deals with those permissions.

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

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

6) Concessions can be on the public, sterile and/or secure side of screening, and may require design accommodations that enable certain users to have access to limited service areas and/or 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 each operator. However, each cargo operation must remain consistent with the Airport Security Program (ASP) and evolving regulatory requirements, particularly screening requirements for cargo to be carried on passenger aircraft.

8) Tenants may or may not be aviation-related organizations, and may or may not have specialized security design requirements, depending on their types of operations and their location in relation to other secured areas and facilities. Some airports have light industrial zones where the main operations occur outside secured areas. However, tenants in such areas may have a continuing need to bring 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, still within the requirements of the Airport Security Program.

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. These areas may be issues for close-in terminal access, or some may be removed to the perimeter.

11) Emergency Response vehicles and personnel might come from dozens of surrounding communities and facilities to provide mutual-aid services in the event of an emergency. This fact drives design considerations for ease of perimeter access, direct routes and access to affected facilities, and quick access to terminal 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 provide a direct path between public and secured areas.

When considering circulation from a security design perspective, it is important to move people quickly and efficiently from one public location to another, and to keep them from moving into any area that is, or leads to, a secured or sterile area. This may involve design solutions such as physically separating 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 appropriate employee access, while not compromising security. Finally, attention must be paid to circulation resulting from emergency operations, so that evacuees are channeled away from secured areas.

c. Utility Infrastructure

Security aspects of the planning, design and architectural considerations that support necessary utilities in the terminal are discussed in IT, Power, Communications & Cabling Infrastructure, as well as measures in access control and surveillance chapters, among others.

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 regarding the standards that must be met. No matter what changes are made to an existing building (renovation and/or expansion), or what features are provided in a newly designed terminal, they must meet all security requirements, both regulatory and operational. Security alterations to an existing building may also be impacted by Building Codes and result in added modifications and increased costs.

An existing building may have physical constraints that make a particular security concept difficult or impossible to retrofit. One example might be a curved or angular concourse that provides very limited lines-of-sight for surveillance. Such constraints may require the designer, in consultation with the airport operator, to choose an operational alternative that may not be the optimal choice. That choice may be further defined by such factors as initial cost and funding sources, short or long term maintenance concerns, compatibility with related 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 drive similar decision-making processes during the design of a new terminal building. The difference is that while the constraints of an existing facility may no longer be a limiting factor, the "clean slate" of a new facility design allows for many more technological and procedural options; each of which may bring many more competing design influences to the table, along with added costs and integration challenges with legacy systems. For example, in updating an 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 technologies. A new facility, however, provides a multitude of options for new vertical or horizontal circulation patterns, new entries and exits, new demands for added terminal building infrastructure requirements (i.e., power, water, HVAC, etc.), and new technologies which may out-perform existing ones and put into motion future plans for upgrades of legacy systems to meet new standards.

In summary, each terminal building project requires a similar decision-making process to determine the appropriate security requirements, and how they are to be applied. This would occur in the development of a Concept of Operations (ConOps), discussed elsewhere in this document, which examines the airport requirements and the available options. 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.

3. Sterile Area

At an airport with a security program under 49 CFR 1542, the "sterile area" of the terminal typically refers to the area between the security screening checkpoint and the loading bridge and/or hold room door leading to the aircraft. The sterile area is controlled by inspecting persons and property in accordance with the TSA screening protocols and TSA-approved airport security program. The primary objective of a sterile area is to provide a passenger containment area, preventing persons in it from gaining access to weapons or contraband after having passed through the security screening checkpoint and prior to boarding an aircraft. General security considerations of the sterile area include:

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

b. Portals, including gates and fire egress doors, must prevent unauthorized entry by any person to the sterile area, and to the secured area, which includes airside and baggage make-up areas. Doors must also comply with applicable local fire and life safety codes and Americans with Disabilities Act (ADA) requirements, among others. Guards are generally an expensive alternative to technology in this application. Discussions with local building and/or life safety code officials should take place early to resolve special design issues, including how to accomplish the securing of fire doors.

c. Sterile areas should be designed and constructed to prevent articles from being passed from non-sterile areas into 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, sterile or public access to suspended walkways or balconies over or adjacent to sterile areas, it is particularly important to consider effective barriers to prevent passing or throwing items into sterile areas.

e. During planning and layout of sterile areas, consideration should 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 multiple daily access into the sterile area from public occupancy areas

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

3) Concessionaire deliveries and supplies should be considered as a part of the planning and design process. Concessionaires are usually located within the sterile areas. Concessionaires and other airport tenants receive deliveries at all times of the day, often from companies whose delivery personnel change frequently and cannot reliably be given keyed or media-controlled access into the sterile areas. Where possible, deliveries of this type should be limited to a non-sterile area and screened using appropriate hand searches or explosives or X-ray detection methods. Where loading docks are employed, they should not be adjacent to critical infrastructure such as HVAC, IT/communication centers, or emergency power generators, etc. The planning process should develop strategies for concessionaire deliveries, storage areas, employee access routes, and free flow. These require adequate attention to security levels to prevent obstructions and patron queuing areas near or in security checkpoint areas, and to eliminate the occurrence of unscreened delivery and concessions personnel within the sterile area. All such screening should take place well away from designated passenger screening areas.

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 screened person inside the sterile area.

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

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, or flow through it easily, and whether they will be comfortable doing so, particularly where they are occupying additional space with roll-on luggage, requiring not only more space for themselves, but more space between passengers. Security requirements are not always compatible with convenience and comfort.

IATA's Airport Development Reference Manual is a good guideline to define levels of service with *Table III-D-1*, with Level C or higher being the typical goal:

There are both qualitative and quantitative components to level of service considerations—whether they will be comfortable, convenient and efficient, and whether the throughput is sufficient to meet peak demands.

Key to this is the variation in bags per passenger, or carry-on items per passengers as they circulate throughout the terminal. There is also variation based on the segment of traffic (e.g., international or domestic) that could lead to more congestion.

For planning guidelines purposes an airport terminal aiming for a good level of service would provide 13 to 22 square feet per passenger for check-in queues. Other systems in the airport (security screening checkpoint queues) could follow similar guidelines, provided adjustments are made for the level of passengers with checked or carry-on bags.

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

Security can be greatly improved by limiting the number of access points to secure areas, 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.

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

Table III-D-1—Levels of Service Definitions

Square Feet Per Passenger	A (excellent)	B	C (good)	D	E
Few carts and few passengers with checked bags	18	15	13	12	10
Many passengers with checked bags (e.g., international), carts and well wishers	28	25	22	20	19

Table III-D-2—Check-in Level of Service

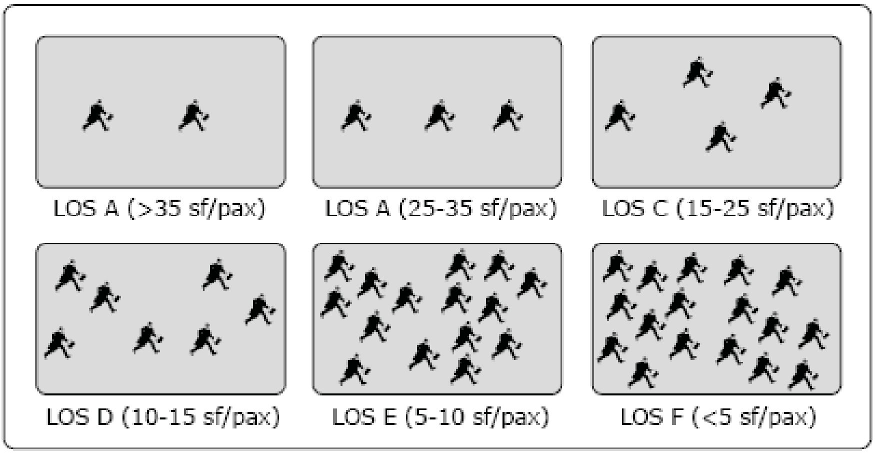


Figure III-D-1—Visual Depiction of Density in Levels of Service in Corridors

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 each successive stage, including curbside check-in, ticket counters, screening checkpoints and vertical transportation to meet peak hour flows. It is necessary to calibrate the capacities of spaces between the various processing elements. For example, the check-in time at the ticket counters should be calibrated by coordinating with the time passengers spend going 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 can be hardened in new designs. Such features as claim areas accessible from the street, bags stored on floors in open areas, and conveyor belts that loop back through curtains into the SIDA, should be eliminated or subjected to heightened surveillance and monitoring.

   In contrast, claim areas for baggage arriving on international flights are completely within the airports' FIS 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, process through Customs and Immigration, and then exit to the public area to leave the terminal. International baggage claim is much less susceptible to unwanted contact or access.

   Airports may want to consider whether the design of baggage claim areas and the routing of arriving passengers should be similar for international and domestic arrivals. (International arrival areas must also accommodate 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 and reconfigured, the secure (international) layout of baggage claim areas can be adapted for domestic arrivals.

Some terminals have designed their arrival passenger flows so that both domestic and international arrivals are channeled directly via secure routings toward their respective 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 unauthorized entry. Segregation of these areas requires a capability to secure or close down sterile areas not in use, and possibly CCTV surveillance coupled with motion detection to maintain vigilance while unattended.

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

If assessments by airport security officials or a prior history of incidents indicate an airport is at increased risk of explosive attacks, planners of new facilities should seek advice from structural and explosives experts. A blast analysis plan (BAP) and vulnerability assessment in accordance with DHS/TSA guidelines may be desirable.

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

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

Careful consideration should be given to the needs of specific aircraft operators, particularly international, who may need to apply additional security measures during the passenger check-in process. Additional queuing, secondary screening and interview 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 inadequately secured access to secured areas.

Consider equipping emergency exit doors with local and/or monitored alarms that can be responded to quickly by staff. The need and location of such emergency exits should be coordinated closely with the local Fire Marshall and/or code compliance 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 should be paid to the potential for problems caused by mass evacuation, whether during an actual emergency or when a concourse may have to be cleared when a breach has occurred. In either case, the designer should seek out optimal paths of travel, bearing in mind that those persons cleared from the terminal will require an area to be held, and possibly require 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 the consequences of false alarms and the need for officer dispatches and other responses to security breaches.

c. Security Doors vs. Fire Doors

Security and safety requirements 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.

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 remain 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; security requirements for the FIS area are included in the CBP Airport Technical Design Standards.

The space planner 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—may be considered in certain limited circumstances, 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 often located throughout an airport terminal facility on both sides of security. It is usually economically advantageous to the airport to make concession areas accessible to the broadest possible range of visitors and passengers. Enhanced security requirements suggest revisiting the balance between locating more concessions in the sterile areas, close to the hold rooms where only passengers are allowed, and placing concessions in public areas ahead of security screening checkpoints, where persons without boarding passes can contribute to the revenue flow.

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 should be carefully planned to facilitate authorized access.

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

Due to the variety of concession types and operations, concessionaires or designated representatives should be involved early in the coordination process... Since concession companies and types can change with some regularity, designers are encouraged to plan flexibly. The needs of advertising concessions, cleaning contractors and private (non-airport) maintenance and repair crews that may serve concessionaires (such as refrigeration contractors or beverage dispensing equipment) should also be considered in the overall security strategy and design.

Critical concession design and planning considerations include the ability to screen personnel and deliveries, the security 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/Internet access, locations of concessions storage and mail areas) that complement these procedural issues can minimize the security risks with proper coordination. A key security risk occurs when deliveries are escorted into the sterile or other security areas and delivery persons may be left unattended, or left to “find their own way out.” While this is a procedural problem, early coordination and planning can provide for design-related solutions such as a staffed visitor/escort sign-in/out station which requires both the escort and escorted to be present both entering and exiting. If the accommodation for such a station is not considered in the design phase, it may be difficult to execute later on.

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 safety and 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 congestion areas, message conflicts, and common nomenclature provide the designer with a basis for programming the signage plan. TSA's own security signage options may be obtained through the FSD. These elements are important to security because they convey information needed to understand the paths of travel available, especially when conditions are changing from normal to emergency mode. A comprehensive information system can help to make the security process more user friendly, particularly among new, 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 such as FIDS and MUFIDS displays. Integrating dynamic signage with the airport's information systems network can give the airport great flexibility in determining what is displayed at any particular location and at any given time.

This flexibility can also serve security purposes, because dynamic signage can provide the means for delivering security information on a timely basis during rapidly changing security events and emergency situations when warnings and instructions for passengers and support personnel are critical. To be effective, these capabilities should be identified early in the planning and design process to 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 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. It is also necessary to be certain of adequate consultation and coordination with groups representing persons with disabilities, and government agencies such as TSA, FAA and FIS; plus those administering local fire and safety codes, etc.

1) Signage-specific coordination will be required for:

    a) Electrical and IT systems (providing power and data to signs);

    b) Video/Cameras (obstructions);

    c) Sprinkler Systems (obstructions);

    d) Lighting (obstructions and/or external illumination of signs); and

    e) Emergency UPS / generator during power loss or evacuation operations.

f. Public Lockers

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

g. Unclaimed Luggage Facilities

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

h. VIP Lounges/Hospitality Suites

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

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.

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, access-controlled, and possibly add surveillance. (Service corridors may be desirable to enhance public aesthetics by concealing service and delivery activities, and can increase airport efficiency by providing clear, unobstructed pathways where airport personnel can quickly traverse the terminal.)

2) Service corridors may also be used to minimize quantity and type of security access points. If access requirements are clustered by similarities of personnel or tenant areas (such as airline ticket offices, concession storage areas, concessionaires, or equipment maintenance access points), a common service corridor may serve multiple entities, and may provide greater control of security than separate access points for each user.

3) The planning and design of non- service corridors should consider their placement and possible use by airport emergency personnel and law enforcement agencies. While use of service corridors by emergency and LEO personnel is not a security requirement, proper corridor placement and design characteristics can enhance response times as well as allow for private, non-disruptive transport of injured persons or security detainees.

4) Vertical circulation and stairwells are more difficult to control than corridors. They provide access not only to multiple floors, but often to multiple security levels as well. In particular, fire stairs typically connect as many of the building's floors/levels as possible. Since they are located primarily to meet code separation requirements and provide egress from the facility, they are not often conveniently located with regard to security boundaries or airport operation. Thus, additional non-fire stairs, escalators and elevators are often needed as well. Optimally, vertical cores are shared for egress and operational movement.

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 support offices, law enforcement, ID offices and security force offices and substations, as well as airline and tenant (including government agency) offices.

Office areas are best located close to the primary activity of the occupants to minimize the need for multiple security transitions. There may be various office areas within multiple security areas depending upon the function and preferences of the airport personnel. Office areas should be located and connected via corridors and vertical circulation, to minimize the amount that the office personnel will need to cross security boundaries in their daily activities. Likewise, office spaces should be planned with consideration for visitors and public access, as well as the likelihood that those visitors might be inadvertently left unattended or unescorted, providing unintended access to security areas.

Consideration should be given where appropriate to the use of satellite police, ID or first aid offices that allow for easy public access and the possibility of more efficient response times.

Other than the considerations of whether office areas are within security areas, or how frequently office personnel will cross security boundaries, the security of the office areas themselves is often an anti-theft and personal safety concern. When airport operator/administration offices are located within a public terminal, these areas are often equipped with security access control equipment and/or monitored by CCTV or patrols. It is typically more cost-effective and efficient to use a single security system for all requirements; these areas usually require security door treatments, duress alarms, and connection to the airport operations center and monitoring equipment.

Additional design considerations include: security of airport personnel and financial records, security of access control and ID workstations, security of identification media stock and records, safe and money storage areas, and computer server and IT/communications equipment areas, especially for security-related facilities such as the access control and CCTV systems.

c. Tenant Spaces

There is no fixed rule on whether tenant spaces require tie-in to the access control system. Indeed, there are currently no such regulatory requirements for tenants to have a security program, although if the airport wishes to include tenant areas, it is wise to design a single unitary system rather than try to integrate multiple tenant systems. This decision necessitates early discussions with each tenant, and perhaps a representative of the tenant community as a whole, to look at such protection requirements as money-handling operations, high-value cargo, overnight cargo and maintenance operations, and late night or early morning concession deliveries, etc.

d. Law Enforcement & Public Safety Areas

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

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.

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 multiple terminal locations to improve response times to widely separated facilities, as well as reduce vulnerability to a single point of attack.

d) Physical infrastructure should consider adequate space for:
i) Communications, surveillance monitoring and IT systems
ii) Briefing/work room
iii) Training classroom/offices
iv) Property/evidence room(s)
v) Conference rooms—can be part of CP/operations room(s)
vi) Holding cell(s)
vii) Satellite locations, if used
viii) Private Interrogation/Witness Statement room(s)/area
ix) Lockers, showers, restrooms and rest facilities

x) General storage areas
xi) Secured arms storage
xii) 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) EMT/Medical services

f) Consideration should 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 National Crime Information Center, FBI, Federal task forces and other liaison, attention should also be given to the amounts of conduit required to accommodate future expansion in this era of rapidly increasing security requirements and government liaison.

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 secured and structurally adequate 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, 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 integrated space.

c) Consider maintaining control of un-issued ID media stock, access control paper records, master keys and key control systems, and the ID office itself by putting them behind a door with a card reader to monitor access to the system and its records, especially during off hours. It is prudent to consider providing secured portals and card readers for any facilities where the airport may wish to have workstations with security system access, particularly where the ID media stock and personnel data may be stored.

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, the number of dogs, and the layout of the airport. If there is no on-site K-9 operation, but the airport has on-call access to teams from other jurisdictions for emergencies, it would be prudent to specify a non-critical area that could be easily 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 daily operational 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 should consider at a minimum:

   a) Adequate ventilation, cooling, heating, and sanitation systems.

   b) Provide isolation from jet fuel fumes, since the dog's sense of smell is critical to its mission.

   c) Minimal noise levels. Kennels must not be located near runways, taxiways, engine test cells, small arms ranges, or other areas where the time weighted overall average sound pressure level for any 24 you period exceeds 75 adjusted decibels.

   d) Areas free of infestations of mosquitoes, ticks, rodents or other pests.

   e) Must be located in an area that will allow for the proper supervision, protection, and care of the canine.

   f) Administrative area should have secured storage for training items such as (luggage, K-9 supplies, etc.).

   g) Storage facilities for Explosives Training Aids, which must be coordinated with the TSA's National Explosives Detection Canine Team Program (NEDCTP) Office and the Department of Justice, Bureau of Alcohol, Tobacco, and Firearms and Explosives (BATF) regulatory requirements.

   h) Also consider reasonable proximity to EOD personnel, as well as adequate parking nearby for K-9 transport vehicles.

6) Service Animal Relief Areas

   a) Service animal relief areas will often include grassy space, drinking water, cleaning capabilities such as water hoses and disposal containers, and appropriate drainage. Generally, maintenance of grassy areas is only practical on the public landside, not airside, but artificial materials may be used for service relief areas located on the sterile side.

   Additional Assistance regarding different kennel designs for various climates or other information regarding kennel facilities is available from the TSA NEDCTP Canine Training & Evaluations Branch.

b) Individuals with disabilities will often be able to use these landside areas for their service animals. However, for transiting/connecting travelers with disabilities, access to landside relief areas may not be possible due to time constraints and disability-related reasons.

In order to allow such travelers access to service animal relief, airports may choose to locate a more limited service animal relief area on the sterile side (for example using artificial materials and with fewer amenities), or may provide travelers with escorted access to non-designated outdoor areas for the purpose of service animal relief.

c) Airports should determine the need for, design, and location of designated Service Animal Relief Areas for use, and the circumstances in which access will instead be afforded to other outdoor areas. For transiting/connecting travelers needing access to those service relief areas located inside the sterile area, an appropriately badged escort will be required.

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, particularly where they may co-locate with other operational functions; such designations may include: Airport Communications Center, Airport Operations Center, or Security Control Center.

An SOC can provide multiple communications links to the airport operator including police, fire, rescue, airport operations, crash/hijack alert, off-airport emergency assistance and a secure communications channel, as well as liaison with Federal agencies. The SOC can serve as the point of integration of all security features and subsystems of the airport security system. Complete and timely detection information can be received at the SOC and used to initiate a prioritized and semi-automated assessment and response.

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

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

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

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

1) Access terminals for law enforcement informational systems such as Computer Aided Dispatch (CAD), National Crime Information Center (NCIC), etc.;

2) Automatic notification system for emergency response recall of personnel;

3) Direct phone lines to ATCT tower, airlines, local hospitals, and other sites, etc.;

4) Airport Emergency Command Post;

5) Fire alarm monitoring;

6) Flight Information Display (FIDS) systems; Baggage Information Display (BIDS) systems;

7) ID management department;

8) Information specialists for customer information lines, courtesy phones, airport paging;

9) Landside/terminal operations;

10) Maintenance control/dispatch or alarm monitoring (includes energy management of HVAC systems);

11) Monitoring of public safety, duress or tenant security alarms;

12) Personnel call-down paging system;

13) Police and/or security department;

14) Radio systems;

15) Recording equipment; and

16) 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 manage separate video and communications channels to two or more highly diverse locations for very different events having dissimilar response requirements.

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 space in adjacent 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, access control and CCTV monitoring.

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, which may include wireless.

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, possibly including wireless.

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 150/5200-31C, 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, preferably airside but in close proximity, should be provided for support vehicles (fire, 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 access controlled, have adequate current and expandable communications links, provide a private and quiet environment, and include space for cots and access to restrooms. Controllable access to the FAC is particularly important to assure the privacy of its users. See the National Transportation Safety Board's family assistance documents.

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. 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.

j. Loading Dock and Delivery Areas

Loading docks and delivery areas are very active areas at airport terminals. Maintenance personnel, vendors and suppliers, delivery vehicles, service vehicles such as trash and recycling and many others use this area 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. Strong attention is also recommended to avoid locating a loading dock adjacent to critical infrastructure and facilities, e.g., IT and communications hubs, emergency power generators, and primary emergency egress portals.

Some airports have chosen to implement off-hour deliveries to lighten truck and van traffic around the airport during the day. 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 paths of travel to recipients, various methods of in-terminal 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, possibly using video analytics, are all potential methods of control.

Space should be allocated and configured to allow for physical inspection of vehicles and their contents. During heightened security conditions, physical inspection, including the under-carriage, of all delivery vehicles approaching the terminal might be required, with consideration for at least temporary vehicle inspection points and holding pens.

Another advantage of controlling vehicle access to the terminal loading dock is the reduction of unnecessary cars and vehicles that may attempt to use the loading dock area as a general temporary parking area. Vehicles left unattended adjacent to the terminal present a risk of vehicle IEDs. CCTV monitoring of parking areas can alert security personnel to vehicles that have been left for extended periods. Consideration should be given to parking areas that are relatively distant from the loading dock/terminal building for extended parking of service and delivery vehicles.

k. Cargo Facilities and Security Considerations

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

1) Overview of Air Cargo

The Transportation Security Administration (TSA) is responsible for ensuring the security of all modes of transportation, including cargo placed aboard passenger and all-cargo aircraft. The Implementing Recommendations of the 9/11 Commission Act of 2007 specifically now requires 100% screening of all cargo to be loaded on passenger aircraft. Part of TSA's missions is to continue to evaluate both near-term and long-term security measures and adjust screening regimens that enable cargo screening throughout the supply chain. Although this document is primarily concerned with designated airport and airline facilities, including secure areas of freight forwarder facilities other cargo shippers certified to tender screened cargo to air carriers can also apply these guidelines.

TSA has adopted security measure throughout the air cargo supply chain that apply to aircraft operators, foreign air carriers, indirect air carriers (freight forwarders), and participants in the Certified Cargo Screening Program (CCSP). Under CCSP, shippers and other entities are allowed to screen cargo at an earlier point in the cargo supply chain, which also has an impact on the planning and design of cargo facilities both on and off the airport. Early coordination with all stakeholders involving facilities where air cargo is sorted, screened, or loaded onto pallets or containers is necessary to ensure that security requirements are addressed.

About 50,000 tons of air cargo is shipped in the United States daily, and of that amount, about one quarter is shipped via domestic passenger air carriers. Thus, given the continuing threats against the aviation sector and air cargo itself, the security considerations during planning and design of cargo facilities are important, as well as varied and complex. The principal considerations revolve around a facility's location and the type of business operating from that facility. In general, there are three types of cargo businesses/facilities: those accepting and processing cargo that will be transported in passenger aircraft; those accepting and processing cargo that will be transported in cargo aircraft (freighters); and those accepting both types of cargo. To meet the screening requirement, another type of cargo facility has evolved from the implementation of the CCSP—the Independent Cargo Screening Facility (ICSF), which is now an option for shippers to screen cargo before tendering the shipment to an air carrier for transport.

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

2) The Cargo Facility's Perimeter

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

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

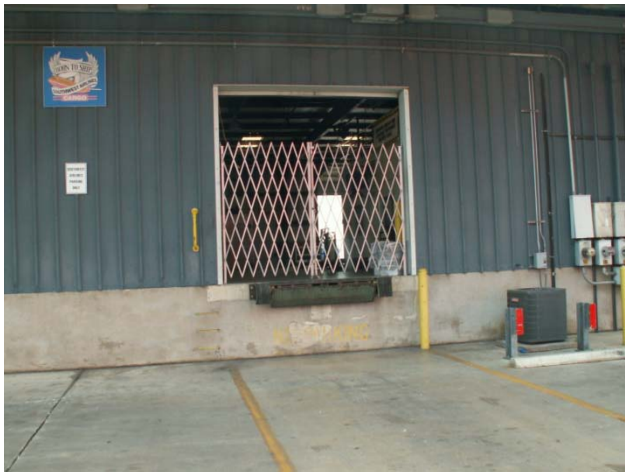


Figure III-D-2

Scissors Gate on Public Side of Building

Also, any authorized personnel doors or gates that permit access to any airside portion of an airport need the appropriate access controls as required in the ASP, as well as requirements for the operation of both airside facing and landside (public side) facing overhead cargo doors. Scissor gates (photo) or other gates installed on the cargo doors facing the public side of the cargo facility permit ventilation when combined with the appropriate procedures to maintain the integrity of the airport perimeter. Appropriate lighting is also necessary around the perimeter of the facility as well as inside the facility.

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

3) Access Control and Monitoring of the Facility

The considerations for the establishment of a facility's access control system and employee credentialing vary widely depending on the type of facility, the location of the facility within the airport environment, the size of the facility, the number of employees and the volume of cargo processed, the number and diversity of carriers, and the airport's size and ASP requirements.

A facility usually faces an airport's AOA/SIDA and has active portals that lead to and from the AOA/SIDA to the interior of the facility, and it must have an access control program or system and an ID badging system described within the airport operator's ASP. The cargo facility's access control system can range from something as simple as a proprietary lock and key management system to an electronic access control system that is a part of or compatible with one used by the airport operator to conform to the requirements of the airport's ASP. The requirements for a lock and key program should be detailed in the ASP. The identification media used could be that used by the airport operator or it could be an identification medium unique to the operator of the cargo facility.

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

Public access to a facility should be limited to a counter area that is separate from the actual warehouse and has direct landside access that allows for the transaction of any business, but prevents unauthorized access to such restricted areas as administrative offices, the ramp, cargo screening areas, and screened or unscreened cargo within the warehouse. Regardless of the type of access control system, the system should be scalable to allow for upgrades to access and monitoring control systems.

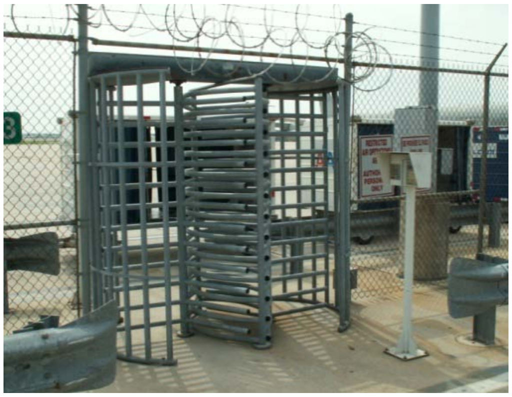


Figure III-D-3

One-way Revolving Personnel Gate

4) Cargo Facility Space Planning and Screening Process

Regardless of the type, size or location of the facility at an airport, consideration for the flow of cargo through a facility needs to be part of the design plan. The flow of cargo, customers, and employees has an impact on the layout and the efficiency of the facility. Cargo handling and control drives the overall allocation of space for movement of shipments from receiving, to screening and cargo consolidation, and ultimately to aircraft loading. Consideration for space includes the storage of cargo that has not been screened, bulk pallet inspections, and secure cargo holding areas. The separation of public access areas within the facility from secured cargo areas needs to be determined; and must ultimately limit access to screened cargo and must be limited only to those authorized personnel. One typical design feature is the establishment of a lobby and reception counter area. Whenever cargo is accepted from the public for shipment, access control points must exist between the counter and any non-public area where cargo is inspected, sorted, and prepared for transport, and accessible only to appropriately badged employees.

Within a cargo facility, cargo should be segregated based on its position in the screening process. Certain cargo may arrive prescreened and ready for loading. This typically may require separate access doors to optimize cargo flows. It should be held with cargo that is received, screened, and palletized at the facility and is awaiting shipment. Both these segments should be segregated from cargo just received or undergoing the screening process. In the event that screening will take place in the cargo facility, additional space allocations should be provided for the breakdown, screening and buildup of cargo pallets and containers. Cargo segregation may also include separating cargo destined for passenger carriers or all-cargo (freighter) carriers; known and unknown shipper cargo, or cargo being transported under a Customs bond. In designing the inside of the facility, planners and designers should give thought to how the screened cargo should be segregated. In certain instances where cargo is transferring directly from one aircraft to another, a separate holding area may be required. In small facilities, a simple demarcation line, conspicuously painted on the ground, may suffice. In larger facilities, the screened cargo may need to be segregated by means of large cages built into the facility with access controls on the portals to prevent tampering. High vertical rack storage will

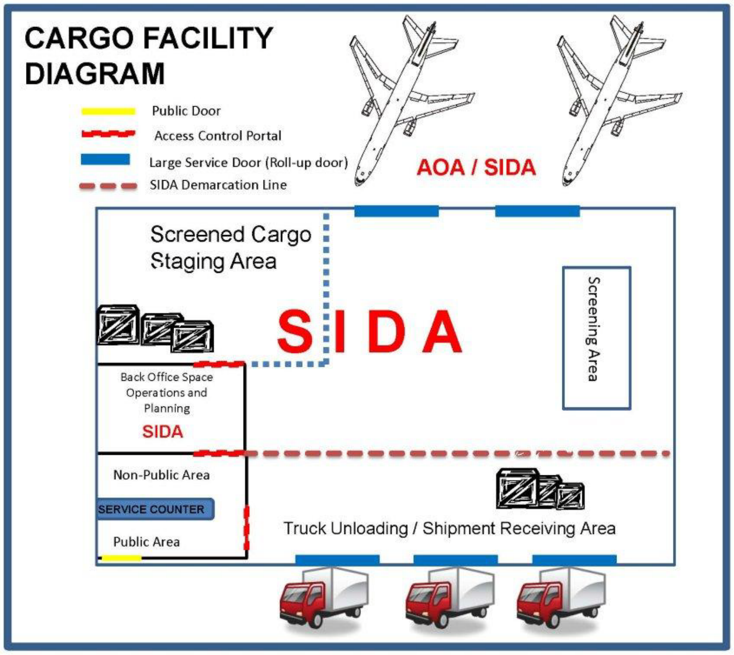
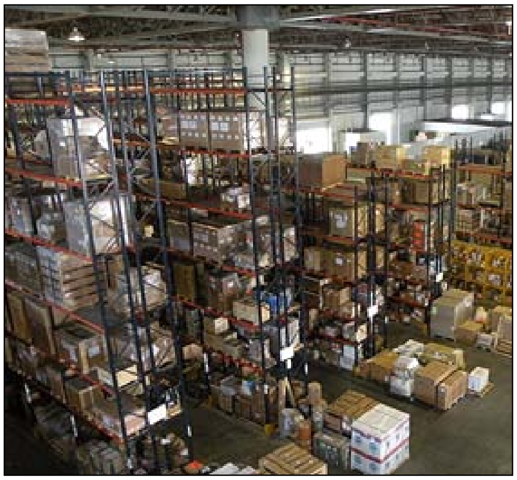


Figure III-D-4

Cargo Facility Diagram

require maneuvering space for tugs and forklifts, and possibly sight lines for high and low lighting and CCTV surveillance. In many new facilities, there is a trend toward common use, i.e., a single building operator for multiple tenants. In such instances the installation of a sophisticated material handling system (MHS) may substantially alter the floor layouts and simplify the routing of cargo and its storage pending delivery to the aircraft or on the inbound side, to the consignees. Special accommodations may be necessary for high value, perishable goods or refrigeration requirements.

Figure III-D-5—Cargo Facility with High Vertical & Wide Aisle Space



5) Surveillance of the Cargo Facility, Its Employees and Its Process

In designing the inside and the outside of the facility, consider the need for Closed Circuit Television (CCTV) surveillance for added security, deterrence, monitoring of processes, proof of regulatory compliance, and forensic evidence. CCTV system requirements and design are covered in considerable detail in the CCTV section of this document. Critical locations for CCTV coverage and appropriate lighting at a cargo facility include:

a) The public side loading dock where large shipments of cargo are accepted;

b) The customer service counter where parcels are accepted from the public;

c) The area where cargo is screened;

d) The areas inside the facility where screened cargo is staged for shipment;

e) The ramp area on the non-public side of the facility;

f) All doors giving access to the airside (AOA/SIDA) of the airport;

g) Any portion of the building that abuts the airport’s perimeter; and

h) Public and employee parking areas.

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

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

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

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

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

a) Delivery Facilities Required

i) Loading Dock: Designed to accommodate the peak drop-off activity, normally early in the morning. The dock should accommodate deliveries by tractor-trailer trucks and step-vans and required material handling equipment. The loading dock platform should be large enough to provide staging for off-loading of product during the receiving process, as well as adequate vehicle circulation. Good lighting for both the outside and inside of the loading dock is necessary. If airport policy requires coverage of the area with CCTV, the lighting levels both outside and inside should be adequate to ensure the effectiveness of the CCTV system. Lighting levels inside the loading dock must be adequate to clearly read package labels and any receiving equipment/system read outs as may be required to verify and inspect deliveries.

ii) Security Processing Equipment: Current TSA regulations require that products destined for SIDA, secured and sterile areas of the airport be inspected. Some airports may require some level of machine screening capability—either now or in the future. It is important that adequate space be provided for the required inspection/screening process during peak receiving hours. Designers should consider what may be required in the future regarding screening and incorporate the flexibility to scale the inspection process to a screening process in the future. Typically this would perhaps require additional space, power and IT capabilities.

iii) Storage Areas: At a minimum, secure temporary storage for received goods needs to be provided in the receiving area so that products can be temporarily stored until delivery to consignees or further air shipment. The airport's receiving process and contracts with their concessionaires and possibly third-party cargo handlers determines how big these storage areas need to be. If the airport and its concessionaires have developed processes to support consolidated receiving of product, and so long as significantly sized long-term storage areas are not located throughout the terminal building, it is quite likely that the most space and manpower efficient solution for storage is to provide consolidated, long-term storage facilities in the receiving area. The storage would need to be sized to accommodate the peak demand for dry, refrigerated, perishable, frozen and high value goods, segmented and secured for each concessionaire, in the SIDA or secured area of the terminal. Once the concessionaire retrieves their goods, they will need to follow the airport's security procedures to ensure that the product remains secure during its transit to their facilities. Depending on the airport's security policies, the need for a continuously secure path may also have a planning/design impact that should be considered. Also, if an airport elects to follow a consolidated receiving and storage philosophy, in order for the airport to reap the productivity benefits of such a policy, it is important that only short-term storage areas be provided in other areas of the terminal adjacent to concessionaires. Otherwise there is the possibility of facility over-sizing and that may not be cost justifiable.

iv) Employee Support Areas: Depending on the size of the receiving/storage area and availability of adjacent facilities, consider the need to incorporate restrooms, break rooms, communications, etc. and other spaces in the design.

v) Other Security Systems: Based on the Airport Security Program, the designer of the consolidated receiving area needs to consider which of these systems are required to be incorporated in the design. These may include access control systems, possibly with biometric enhancements, CCTV systems, and passive surveillance systems.

b) Summary

These recommendations are based on a report performed for the TSA and National Safe Skies Alliance. The overarching conclusion is that to the extent possible, designers should reduce the number of delivery portals to sterile and secured/SIDA areas to the absolute minimum number possible based on the airport's physical configuration. Consolidating all deliveries to a specific location or a reduced number of locations to streamline the operation, increase ramp safety and security and reduce inspection costs should be the ultimate goal. Especially with respect to receiving operations, designers should consider that any processes or practices that can be standardized will produce both operational and cost benefits as well as increased levels of safety and security.

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 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 operator'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 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; they are part of a complex, integrated series of facilities that provide the basic and varied services of a modern airport. There are other areas outside the terminal where both terminal and overall airport security may be compromised.

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

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

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

The terminal also may have walkway or bridge connections to other terminals, hotels, parking structures or other airport facilities and structures, including underground paths. Security strategies should 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 significant vulnerability. The planning and design of these systems should consider not only terminal security, but where the conveyances cross through or above portions of the airside and landside.

8. Chemical and Biological Threats

Airport planners should be cognizant of the potential of chemical and biological threats to their facilities. A chem/bio attack can be viewed as use of a weapon of mass destruction with significant economic impact. The development of appropriate facility and procedural responses to a potential chem/bio attack will provide an effective response to any of several chem/bio scenarios. It is possible that the airport visitors, passengers and staff could be threatened by a non-terrorist accidental release of volatile inhalation of hazardous industrial chemicals like chlorine or ammonia. This release could happen off airport property but require appropriate facility HVAC management and that personnel shelter in place.

The public area may be exposed to a perceived or actual noxious chemical release, perhaps an abandoned leaking pepper spray container or items confiscated at checkpoints, which will require assessment, limited evacuation, mitigation and removal. An actual chem/bio agent released in the public area might also require decontamination of people and facilities as well as appropriate medical treatment. Preparation and appropriate responses to all of these scenarios will minimize any injury to passengers and staff and return the terminal to operation in a timely fashion. Historically, terrorist-placed devices have been small and of limited effectiveness, but their publicity, economic impact and facility disruption have been significant. Facilities can be contaminated and out of economic production for a year. It is conceivable that a chem/bio attack could be launched against any element of an airport to disrupt the overall operation; however the passenger terminal is seen as the most likely target.

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

- To deter attacks through HVAC system physical security; and
- 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 or biological agent introduced into the HVAC system could involve substantial effort and cost. The first step is to identify those groups that should be involved in the 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 be taken in the event that a suspected attack is discovered. These might include evacuation, triage, quarantine facilities, detoxification facilities, medical mutual aid response capabilities, and screening of vehicles, among others.

One consideration is the use of chemical and biological detection systems for building protection. There are two types of systems currently in operational use. Chemical sensors that can detect some classes of volatile chemical agents are deployed operationally to provide early warning of chemical releases and to enable rapid and effective facility responses. Such a system has been in operation in the Washington, D.C., Metro for several years. As of publication time, real-time bio-detection 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 real time responses, but does allow exposed individuals to be identified within a few days and treated before they become ill, significantly improving their chances of survival. Such post attack detection also allows contaminated facilities to be identified and isolated, preventing additional exposures and additional spreading of contamination. Airport operators should explore the potential uses of available detection technologies 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” 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 attack, given the technologies and capabilities available at the time. With the report, airport planners should gain an understanding of the important issues for chem/bio preparedness, and should be able to assess the status of their airport to determine whether to bring in consultant expertise, and to target the most effective upgrades for their facilities. The report has been distributed by the Transportation Security Administration (TSA) to Federal Security Directors at the high threat airports, and by the Airports Council International and the American Association of Airport Executives to airport executives and security planners.

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

□ **Design to be flexible; technology & regulations change**

□ **Coordinate access points, minimize crossing security boundaries**

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

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

□ **Limited Concealment Areas/Structures**
- Minimize concealment areas
- Minimize and lock accessible spaces

□ **Different Operational Pathways for:**
- Passengers & Airport Personnel
- Tenants / Concessions
- Emergency Response Routes
- Delivery Routes
- Security Response; Police Escorts

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

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

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

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

- □ **Meet with all relevant airport users and stakeholders, including tenants and government agencies, to determine user requirements documented in ConOps.**
- □ **Concerns about personnel circulation include 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**
  - Area between the security screening checkpoint and door to aircraft.
  - Objective: passenger containment, prevent access to contraband
  - Number of access portals limited to minimum operational necessity
  - Comply with local fire/life safety codes, Americans with Disabilities Act (ADA)
    - Prevent articles from being passed from to sterile or secured areas
    - Consider paths of access in restrooms, airline lounges, kitchens, plumbing chases, air vents, drains, trash chutes, utility tunnels or other channels
    - Consider multiple access needs of airport, airline, maintenance, tenant and concession staff
  - Emergency response routes
  - Routes for access by off-airport response, ARFF/fire, emergency medical services [EMS]
  - 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 number of access points
    - Monitor portals and conveyors via CCTV
    - Furnishings—avoid concealment of explosives
    - Seek structural advice on minimizing blast effects
    - Ticketing Lobby
      - Minimal seating to reduce congestion
      - International operators have extended security measures
      - Additional queuing space may be required
  - Public Emergency Exits
    - Code requirements; coordinate with Fire Marshall
    - Avoid moving persons from lower to higher security
    - Consider push-type bars with 15-30 second delays
  - Concessions Areas
    - Consider temporary move during heightened security
    - Short delivery routes that minimize crossing security boundaries
    - Consider type of concession needs: storage, high-value items, ATM security.
  - Prevent public access to the airside by connecting elevators, stairwells
  - Signage: Types of agencies with interests in signage at airports:
  - Federal Inspection Services
    - infrastructure required for power and data to signs, surveillance, lighting
  - Lockers:
    - Eliminate public area lockers

- Unclaimed luggage areas—landside, with EOD / LEO access
- VIP Lounges/Hospitality Suites
    - Consider location in relationship to sterile area access
    - Provide space for monitored baggage holding facilities
- Observation decks discouraged

Section III-D-5—Nonpublic Areas Checklist:

□ **Non-Public Areas**

- Service Corridors, Stairwells and Vertical Circulation
    - Minimize access points, do not cross secure boundaries
    - Tenant areas grouped in common service corridor
    - Consider needs of emergency/LEO personnel
    - Stairwells, vertical pathways may require security treatments
- Airport Personnel Offices
    - Minimize need to cross security boundaries
    - Planned to accommodate public access
    - Consider satellite police sub-stations, ID or first aid offices
- Tenant Spaces
    - Some may require tie-in to airport access control and alarm system
    - Consider tenant money-handling, overnight operations, off-peak deliveries
- Law Enforcement & Public Safety Areas
    - Public Safety or Police Offices
        - Office space in the terminal—consider communications links.
        - Protected with ballistic materials, bollards, etc.
        - Public access to administrative, ID offices, Lost and found, training rooms, EMT
    - Law Enforcement Parking—direct landside/SIDA access
    - Remote Law Enforcement/Public Safety Posts/Areas, substations; outdoor shelters
- Dogs/K-9 Teams
    - Specify non-critical area for K-9 use
    - Rule of thumb: 4-by-8-foot indoor pen, outdoor fenced exercise run
    - Plumbing and drainage; epoxy coated floor for cleaning
    - Fresh air circulation, dry, no mildew or dampness
    - Secured, isolated from casual public contact
    - Isolation from noise and odor sources, especially jet fuel fumes
    - Secured storage for explosives test and training items; coordinated with ATF
- Security Operations Center (SOC)
    - Multiple communications needs for police, fire, rescue, airport operations, crash/hijack alert, off-airport emergency assistance,
    - Locate close to the Airport Emergency Command Post (CP)
    - Central cabling interconnections, reasonable cable lengths
    - Rear access to console for maintenance
    - Consider space requirements for consolidating all LEO functions in SOC:
    - Plan an alternate site for basic operation.
    - Direct view of the airside and isolated parking
    - Other Considerations
        - Raised flooring installation of ducts and cable paths
        - CP electrical power must be uninterrupted
        - Vehicular access, for support vehicles and key CP vehicles
        - Space for kitchenette and rest areas
- Family Assistance Center—access-controlled space.
- Loading Dock & Delivery Areas
    - Access control and identification media
    - Package screening
    - CCTV
- FIS Areas
    - FIS agencies publish a separate document

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

□ **Due to the complex/multi-use function of public terminals, they contain the broadest range of vulnerable areas**

□ **Each airport is unique and should be evaluated for unique or increased vulnerabilities**

□ **Terminal Vulnerable Areas**
- Connections from the terminal to utility services in power and communications
- Hotels, parking structures or other on-site or adjacent public facilities and structures
- Loading docks and delivery areas
- Locations for person or object concealment
- People moving systems, if exposed, including underground and elevated rail
- Primary transformers, switching gear and UPS
- Secondary generating equipment and transmission facilities
- Utility tunnels or ducts entering a terminal below grade
- Voice and data switching and transmission facilities
- Walkway or bridge connections to other terminals

Section III-D-7—Cargo Facility Checklist:

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

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

□ **Surveillance—Critical CCTV locations include:**
- Public side loading dock
- Customer service counter
- Cargo screening areas
- Staging areas
- Non-public ramp area
- All access doors to AOA/SIDA
- Public and employee parking areas

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

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

Section E—Baggage Systems

1. Introduction

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

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

The main topics covered here are:

a. CBIS Overview;
b. Federal Funding Options for CBIS Design and Construction;
c. Principles for CBIS Planning and Design;
d. Roles and Responsibilities;
e. CBIS and Screening System Types;
f. Development and Evaluation of Alternatives;
g. CBIS Design Standards; and
h. Checked Baggage Resolution Area (CBRA) Design Standards.

2. CBIS Overview

There are two broad categories of CBIS: stand-alone and in-line. A stand-alone CBIS is a system that is not integrated into the baggage handling system; an in-line CBIS is integrated into the baggage handling system. The planning and design of in-line CBISs is the most complex and therefore the focus of this preliminary guidance as well as the PGDS.

An in-line CBIS is defined as the entire system from the point of bag induction, through the Explosives Detection Systems (EDS) screening area, to the point where bags are delivered to the airlines' outbound sortation or makeup system.

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

The process involves the following three screening levels:

a. **Level 1 screening** is performed with EDS units. All bags that can physically fit in an EDS unit are directed to Level 1 screening and scanned using an EDS. All bags that automatically alarm at Level 1 are subject to Level 2 screening.

b. During **Level 2 screening**, TSA personnel view alarm bag images captured during the Level 1 EDS scan, and clear any bags whose status can be resolved visually. This process is referred to as On-Screen Resolution (OSR) which, for in-line systems, allows the continuous flow of bags through the system until a decision is made. OSR typically occurs in a remote screening area. All bags that cannot be resolved at Level 2, and all bags that cannot be directed to Level 1 because of size restrictions, are sent to Level 3 screening.

c. **Level 3 screening** is performed manually and involves opening the bag and the use of Electronic Explosives Trace Detection (ETD) technology. Bags that do not pass Level 3 screening (typically, a small percentage of total bags) are either resolved or disposed of by a local law enforcement officer.

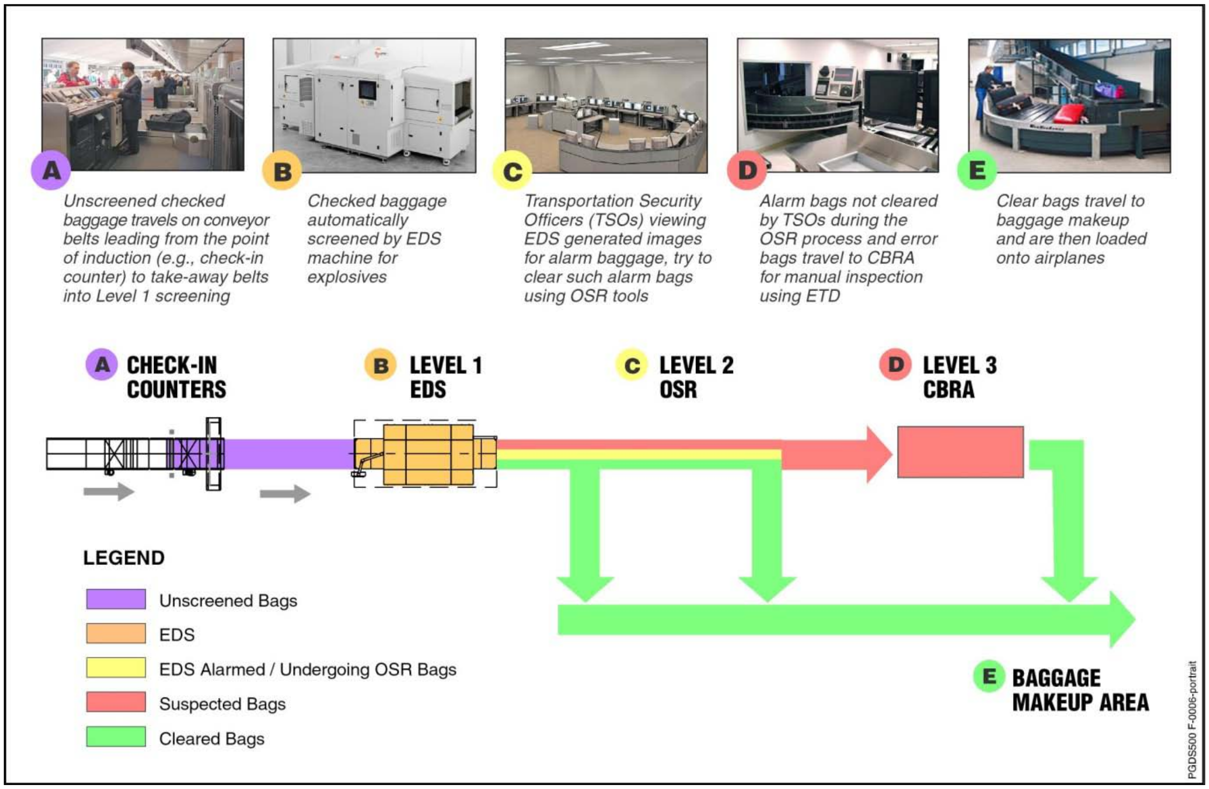

A
Unscreened checked baggage travels on conveyor belts leading from the point of induction (e.g., check-in counter) to take-away belts into Level 1 screening
B
Checked baggage automatically screened by EDS machine for explosives
C
Transportation Security Officers (TSOs) viewing EDS generated images for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

Figure III-E-1—Overview of an In-Line Checked Baggage Inspection System

3. Federal Funding Options for CBIS Design and Construction

TSA, through its Electronic Baggage Screening Program (EBSP), is responsible for the deployment and installation of EDS equipment at airports across the nation. Currently, the EBSP offers two types of Federal funding support to project sponsors:

a. Design Other Transaction Agreements (OTAs)—Funding support for the design phases of a CBIS project

b. Construction OTAs and Letters of Intent (LOIs)—Funding support for facility modifications during construction

Funded systems must comply with the latest published version of TSA’s PGDS.

a. Design OTAs

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

2) Prior to execution of a Design OTA, EBSP will provide rule of thumb guidance on design costs to TSA Office of Acquisition for use in negotiating Design OTAs. TSA will provide the airport operator with optimal systems specifications, including information on equipment counts and the type of system

selected by the Integrated Deployment Model. This information will serve as a starting point for the alternatives analysis to be performed by the airport. Airport operators will be asked to submit a notional schedule for the design effort to support EBSPs planning efforts.

b. Construction OTAs and LOIs

1) Beginning with applications for Federal Fiscal Year 2011 funding and continuing thereafter, project sponsors applying for facility modification funding will be required to have obtained TSA approval of the Basis of Design Report as defined in the PGDS (i.e., to have successfully completed the Schematic Design Phase) to be eligible for facility modification funding.

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

3) Project sponsors will be strongly encouraged to coordinate with local TSA and headquarters TSA via Regional Deployment Managers as early as possible when EDS projects are being considered and conceptually planned. Early notification assists TSA in justifying Federal funding for the Electronic Baggage Screening Program (EBSP).

c. Reimbursable and Non-reimbursable Costs

TSA will only fund those construction costs directly necessary to implement an EDS screening solution and support the OSR room and the CBRA. TSA will identify those portions of the BHS design required to meet TSA screening requirements, as outlined in the most current version of the PGDS. For a detailed discussion on which costs are defined as "reimbursable" and "non-reimbursable" and how costs should be estimated, the reader should refer to the latest version of the PGDS.

4. Principles for CBIS Planning and Design

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

a. Achieve the lowest-cost solution. Achieving the lowest-cost solution requires:

1) assuming implementation of soon-to-be-certified screening technologies during the development of alternatives,

2) considering a wide range of alternatives rather than relying on a preconceived notion regarding which system would be best suited for a particular airport/terminal, and

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

b. Follow design standards. Design standards should be considered throughout the planning and design process and should be met during implementation via system testing but also during planning and design.

c. Understand the complexity of in-line screening systems. Baggage screening systems are complex, especially those with high levels of automation. Many different technologies for conveyance, tracking, and screening must all work together seamlessly to achieve an effective, efficient and reliable CBIS.

d. Appropriately estimate demand and equipment requirements. The approach used to estimate demand and equipment needs for the initial system has a major effect on project costs. The PGDS provides a recommended approach to estimate demand and equipment needs, and clarifies the design year for various components of the CBIS—e.g., for screening equipment sizing the design year is five years beyond the date of beneficial use. The level of upfront investment to accommodate demand beyond the date of beneficial use plus five years should be assessed using a 20 year life-cycle cost analysis.

e. Consider how the CBIS will operate during contingency operations. The best approach for providing redundancy and establishing contingency operations will vary significantly depending on local conditions. In general, low-cost opportunities to "share" capacity across screening zones should be pursued before capacity is added to a specific zone. Regardless of the redundancies built into a particular system, a contingency plan should be developed with the consensus of key stakeholders, including airport and airline personnel, which defines how the CBIS will operate when screening equipment is unavailable, demand exceeds capacity, or a catastrophic system failure occurs.

f. Provide flexibility in baggage screening system designs and facilities. Building in flexibility from the outset to accommodate future upgraded security technologies will keep future upgrade costs to a minimum while maximizing both current and future Explosives Detection System (EDS) performance. Given the rapidly changing nature of screening technologies and the threats facing the aviation system, flexible system design is crucial for successful implementation.

g. Involve all relevant stakeholders. Stakeholder involvement is the key to successful and cost-effective CBIS implementation. This involvement needs to occur at both the industry/Federal government level and the local/airport level.

h. Understand reimbursable and non-reimbursable costs. It may be prudent to gain a good understanding of allowable costs associated with CBIS is imperative when seeking TSA funding.

5. Roles and Responsibilities

The following paragraphs summarize the roles and responsibilities involved in planning, design and implementation of a CBIS.

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

1) Airport—Engineering, operations, information technology (IT), maintenance, planning and design, project management, and others, as appropriate.

2) Airline(s)—Headquarters, operations, corporate real estate, IT, maintenance, engineering, planning, security technology officer(s), station manager(s), and others, as appropriate.

3) TSA—Federal Security Director (FSD), Regional Deployment Manager, occupational health and safety representative and/or other technical representatives designated by the FSD, and TSA Headquarters design review team from the Engineering division with the DHS Office of Security Technology.

4) Additional stakeholders—Local law enforcement and EDS equipment providers and manufacturers.

b. Integrated local design team. As part of the design process, an Integrated Local Design Team (ILDT) that includes representatives of some or all of the above-mentioned stakeholders should be formed. In addition, the ILDT should include a professional planning and design team comprised of architects, engineers, planners, CBIS designers, cost estimators, and project managers. The design team is also likely to include specialty consultants, such as simulation analysts and landscape architects, on an as needed basis. The ILDT is responsible for the development of alternative screening concepts, evaluation of those concepts, and generation of design drawings/submittals. In addition, the ILDT is also responsible for the assessment of specific local conditions affecting the CBIS design, as well as the standards to be met by the design.

c. Project sponsor. The project sponsor is assumed to be an airport owner/operator or an airline (if the system is for an airline-owned terminal). The project sponsor is responsible for initiation and execution of CBIS planning and design, formation of the ILDT, selection of a professional planning and design team, application for TSA or other funding, initiation and execution of construction, as well as testing and commissioning of the CBIS, and operation and maintenance of the baggage handling system (BHS) portion of the CBIS.

d. TSA Headquarters. Representatives from TSA Headquarters are responsible for reviewing and approving/rejecting design submittals. TSA will determine funding eligibility and prioritization as well as assess issues related to occupational safety, health, and the environment. In addition, TSA will determine and provide the specific EDS equipment type to be used and schedule the testing and commissioning of the equipment.

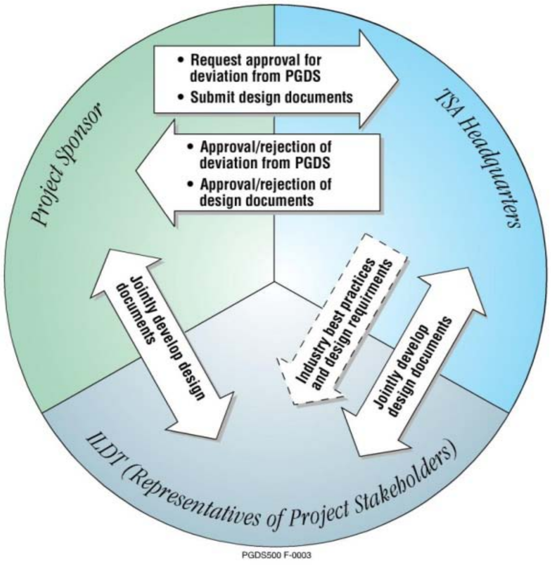

Project Sponsor
TSA Headquarters
• Request approval for deviation from PGDS
• Submit design documents
• Approval/rejection of deviation from PGDS
• Approval/rejection of design documents
Jointly develop design documents
Industry best practices and design requirments
Jointly develop design documents
ILDT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

Figure III-E-2

Summary of Responsibilities during the Design Process

Figure III-E-2 summarizes the interactions between the project sponsor, ILDT, and TSA Headquarters.

6. CBIS and Screening System Types

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

a. System Type 1: High-Volume In-Line CBIS

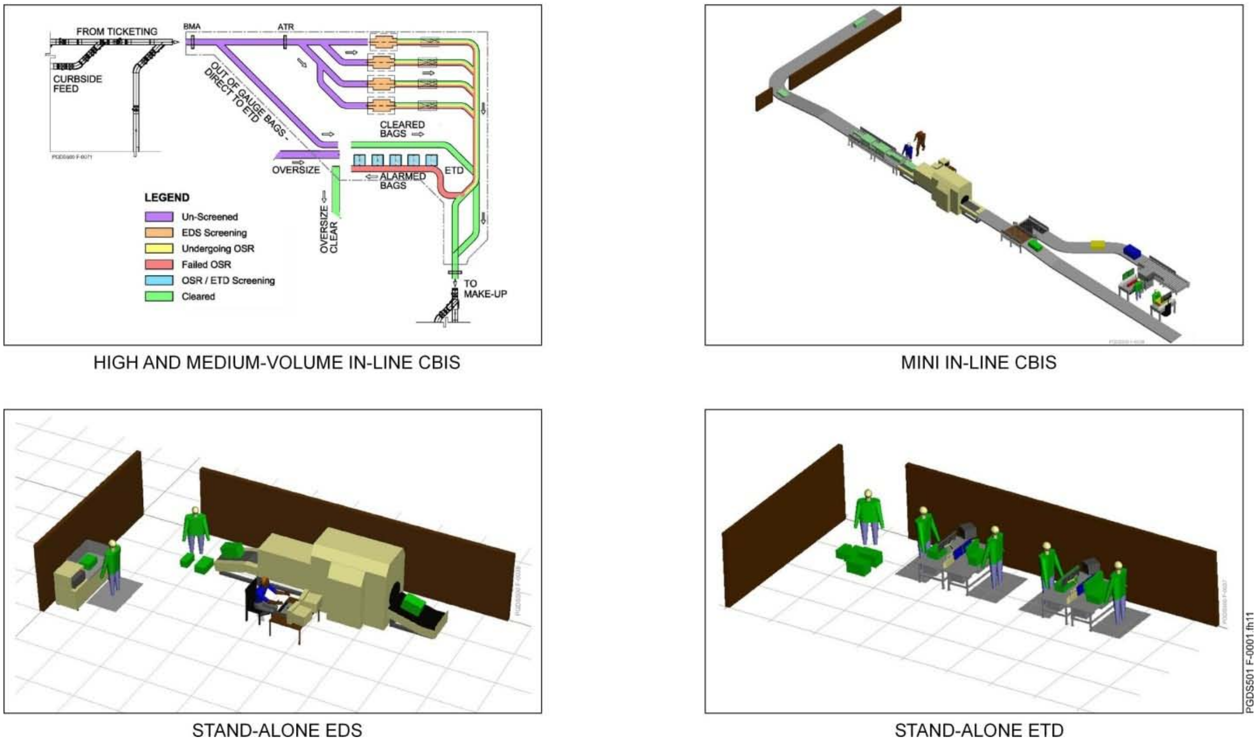
In-line systems using high-volume EDS machines are assumed to have a very high level of integration and a sophisticated in-line conveyor infrastructure, providing sufficient queuing capacity and OSR circulation time while maintaining high throughput and accurate bag tracking. These systems are assumed to have multiplexed EDS technology (i.e., the capability of linking multiple EDS machines with multiple viewing stations), centralized control room(s), OSR capability, a purge line, multiple baggage inputs, and CBRAs. These systems require automated baggage sortation. High-volume EDS machines are estimated to achieve at least a throughput of 900 bph with a low false alarm rate.

b. System Type 2: Medium-Volume In-Line CBIS

This system type includes the existing in-line systems, in which current generation EDS machines are used. These systems typically have multiplexed EDS technology, relatively complex baggage handling system(s), control room(s) (central or local), OSR capability, a purge line, single or multiple baggage inputs, and CBRAs. Upfront capital costs can be reduced by using EDS machines with throughput rates ranging from 500 to 700 bph, as this range would allow for a reduction in the conveyor system size and complexity (compared to high-volume in-line systems).

c. System Type 3: Mini In-Line CBIS

A mini in-line system would typically incorporate a simpler conveyor design and require a smaller footprint. These systems can be located closer to airline ticket counters or baggage makeup devices, which can help reduce travel time and the likelihood of improper baggage sortation. A mini in-line system should be located on the takeaway belt in the baggage room or in the Airline Ticket Office (ATO) area and should include only one or two EDS machines to minimize system integration costs. Because of the decentralized



HIGH AND MEDIUM-VOLUME IN-LINE CBIS

MINI IN-LINE CBIS

STAND-ALONE EDS

STAND-ALONE ETD

Figure III-E-3—Checked Baggage Inspection System Types

nature of these systems, staff and equipment needs would generally be higher than for centralized systems (such as in-line systems using high-volume or medium-volume EDS); however, upfront capital costs would be significantly lower. The mini in-line system would reduce upfront capital costs by using EDS machines with throughputs assumed to range from 100 to 400 bph in locations where no economic justification exists to design and implement a higher capacity in-line system. Typically with mini in-line systems, a centralized OSR room is not as staff efficient as using combined OSR/ETD operations.

d. System Type 4: Stand-Alone EDS

In small airports or in specific zones with low baggage volumes at larger airports, stand-alone EDS may be the most cost-effective option. A stand-alone EDS operates in a manner similar to lobby screening installed today at many Category X and Category I airports; however, where possible, stand-alone equipment should be installed in baggage makeup areas or other appropriate locations to reduce lobby congestion. EDS machines are estimated to achieve throughputs ranging from 100 to 200 bph. This screening system type is relatively labor intensive, but minimal capital investment is required to install the system and support the operation. In some stand-alone systems, combined OSR/ETD can be used.

e. System Type 5: Stand-Alone ETD Systems

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

1) Primary Screening

For security and operational reasons, TSA's goal is to deploy EDS at all Category X-III airports, eventually replacing ETD equipment for primary screening. As such, primary screening with ETD will be used only to screen oversized, fragile, and other baggage that cannot be screened using EDS. ETD primary screening may still be used at smaller Category IV airports. A stand-alone ETD device typically has a throughput on the order of 33 bph per screener (66 bph per ETD machine shared by two screeners).

2) EDS Alarm Resolution

ETD equipment is used to screen EDS-alarmed bags that have not been cleared by screeners using an OSR protocol (based on viewing bag images). This method is referred to as directed trace (or directed search using ETD) and is focused on identifying and locating objects within baggage that have triggered EDS alarms. A typical throughput using this method is 24.2 bph per screener (a national average based on a mix of international and domestic bags of varying sizes, types, and content). Designers should verify this throughput with TSA. For some mini in-line configurations, a more staff efficient method of using directed trace can be achieved by using a combined OSR/ETD method. A typical throughput when using a combined OSR/ETD method is 34 to 45 bph per screener depending on the ETD model

Detailed information on current EDS and ETD equipment models is provided in Chapter 3 of the PGDS. This includes information regarding:

a) Spatial dimensions
b) False alarm rates and OSR clear rates (considered to be Sensitive Security Information available via request to TSA)
c) Environmental operating envelope
d) Weight and floor loading
e) Maximum bag size allowed and average percent out of gauge
f) Expected life span
g) Current procurement status (whether the machine is in development, certified but not yet available for procurement, or available for procurement)

7. Development and Evaluation of Alternatives

Figure III-E-4 summarizes the alternatives development and evaluation process to be carried out during the pre-design/planning.

Planners should develop screening alternatives that account for the following:

a. Airport Spatial Data—Terminal configurations, airline assignments, and architectural constraints.

b. CBIS Capacity Data—Data related to the type of screening systems and screening equipment.

c. Baggage Screening Demand Data—Factors affecting current and future baggage flow into the CBIS, such as existing infrastructure including ticket counter and curbside check-in positions, numbers of gates, and runway capacities.

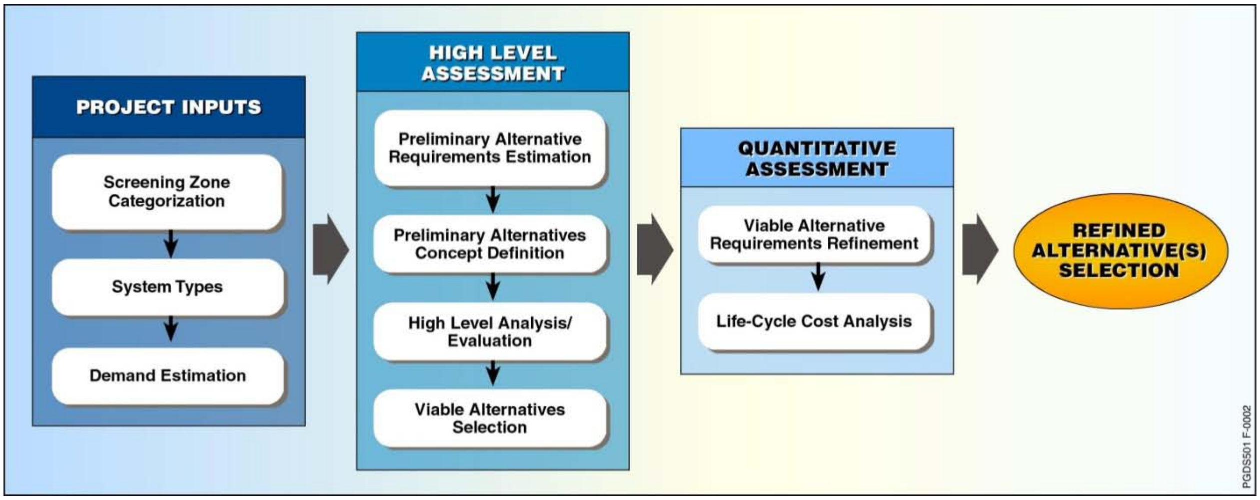

PROJECT INPUTS
Screening Zone Categorization
System Types
Demand Estimation
HIGH LEVEL ASSESSMENT
Preliminary Alternative Requirements Estimation
Preliminary Alternatives Concept Definition
High Level Analysis/ Evaluation
Viable Alternatives Selection
QUANTITATIVE ASSESSMENT
Viable Alternative Requirements Refinement
Life-Cycle Cost Analysis
REFINED ALTERNATIVE(S) SELECTION
PGDS501 F-0002

Figure III-E-4—Alternatives Development and Evaluation

d. Cost Data—Equipment, infrastructure, O&M, and staffing costs.

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

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

8. CBIS Design Standards

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

9. Checked Baggage Resolution Area (CBRA) Design Standards

A CBRA provides the space and equipment required by Transportation Security Officers (TSOs) to conduct:

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

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

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

Section III-E-1—Baggage Screening Checklist:

□ **Refer to TSA Design Guidance Document**
- PGDS standards
- CBRA standards

□ **Funding design and construction**
- Look for low cost solution
- Involve all stakeholders

□ **Three screening levels**
- Level 1–All bags that fit in EDS
- Level 2–Alarmed bags to OSR
- Level 3–Unresolved bag search

□ **Protocols and Concept of Operations**

□ **Checked Baggage Screening Options**
- Fully Integrated In-Line Systems
- Ticket Counter Lobby Systems
- Stand-Alone EDS/ ETD Systems

□ **Airport-specific alternatives—consider:**
- Airport configuration constraints
- IT / space / power / HVAC / floor loading
- CBIS equipment capacity
- Screening demand data–throughput
- Cost–infrastructure, O&M, staff

□ **EDS/ETD Key Performance Characteristics**
- Understand complexity of systems
- Understand non-reimbursable costs
- Flexibility to accommodate change

□ **Consider contingency operations**
- Impact of Threat Levels
- Temporary space for bag staging
- CBRA search area(s)
- Suspect bag retention/removal area

□ **Vehicle access (e.g., Tug, police vehicle)**

Section F—Passenger Screening Checkpoint

1. Passenger Security Screening Checkpoints (SSCP)

The intent of this document is to provide a description of the Security Screening Checkpoint (SSCP) equipment that exists today and the knowledge necessary to locate that equipment within the checkpoint in order to provide the highest level of security screening and efficiency beginning at the queue and continuing through the composure area. The information included in this document should be used when designing new checkpoints or reconfiguring existing checkpoints. All designs and reconfigurations must be coordinated with TSA Headquarters (TSA HQ), the local FSD and staff, and local airport stakeholders so that the recommended guidelines are site-adapted for each checkpoint. For specifics, review the most recent version of the TSA Checkpoint Design Guide Standards (CDGS).

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

This section will address the following issues:

- General Overview of SSCP
- Regulations and Guidelines
- Essential Coordination
- Planning Considerations
- Elements of the SSCP
- SSCP Power & Data
- Safety
- SSCP Project Funding
- Designing for the Future

a. General Overview of SSCP

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

Security screening is intended to deter and prevent hijackings and the transport of explosive, incendiary or dangerous substances or unauthorized weapons aboard commercial aircraft. This threat does not solely rest with the ticketed passengers. Airport and airline personnel, concession employees, and concession delivery personnel may also be part of the threat consideration and are screened through the SSCP when traveling from unsecured areas to the sterile area.

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

1) Preventing persons with prohibited items to board commercial aircraft;
2) Preventing SSCP exit lane breaches;
3) Secure exit lanes for arriving passengers during both operational and non-operational hours of the SSCP;

4) Persons with disabilities requiring wheelchair accessibility or allowances for other assistive devices;

5) Minimal interruption or delay to the flow of passengers and others being screened;

6) Effective and secure handling of tenant goods that cross from the non-sterile area to the sterile area;

7) Equipment maintenance and interference spacing requirements;

8) Operational flexibility in response to changes in passenger loads, equipment, operational processes, and security levels;

9) Flexibility to accommodate new technology and processes;

10) Efficient and effective use of terminal space;

11) Acceptable and comfortable environmental factors, such as air temperature, humidity, air quality, lighting, and noise;

12) Safe and ergonomic design; and

13) Coordination of power, data, and CCTV equipment at the SSCP.

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. Virtually all TSA regulations can be obtained on the TSA Web page.

c. Essential Coordination

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

d. Planning Considerations

TSA equipment placement is intended to increase the level of security and improve the flow of passengers through the checkpoint. This is accomplished by providing adequate space for queuing of passengers, to divest, and compose which minimizes the occurrence of bottlenecks at the checkpoint. TSA HQ and airport designers will collaborate to design to the latest TSA Checkpoint Design Guide Standards.

SSCPs are created by combining standard 1 and 2 lane module sets. These module sets are created based on standard TSA spacing for passenger ingress/egress, clearance for maintenance activities, and prevention of passenger breaches. *Figure III-F-1* illustrates a 5 lane layout which is the combination of two “2-1” module sets and a “1-1” module set. These module sets provide a controlled and contained screening environment where sterile and non-sterile areas are separated from each other.

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

1) Capacity—Number of gates; number of passenger enplanements per aircraft (based on aircraft size and 100 percent load factor)

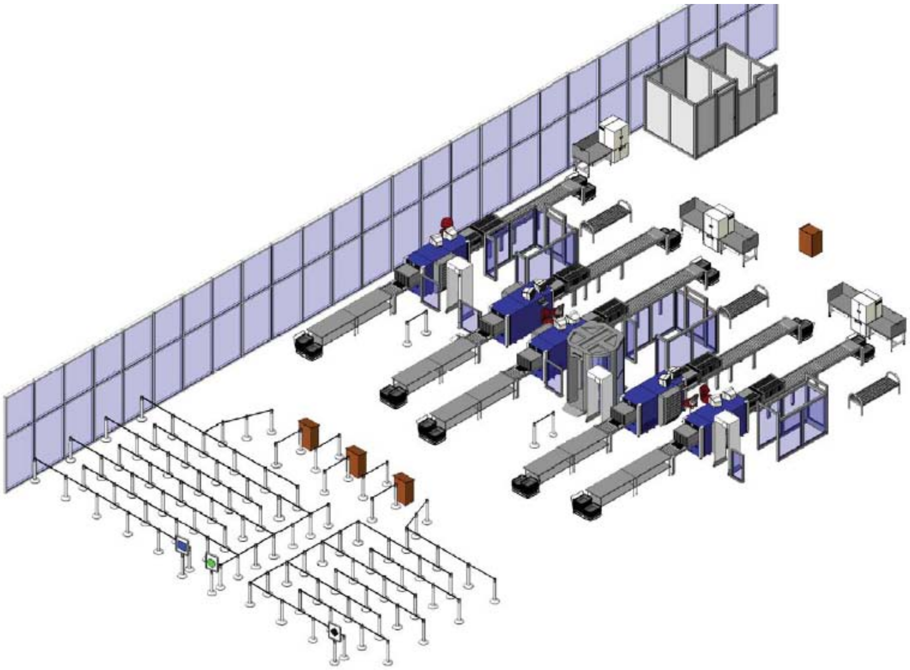


Figure III-F-1—Standard SSCP Layout

2) Passenger Arrival Distribution—Based on the capacity analysis above, determine highest hourly peak rate of enplanements (flight schedules)

3) SSCP Rates & Standards—Based on the arrival distribution analysis, divide that number by the current SSCP Rates & Standards for performance (Local TSA will be able to provide the most up-to-date numbers)

As the number of enplanements per year increases and the equipment and technology evolve, the SSCP needs to have the flexibility for change and the ability to expand. Allowance for modifications should be included in the Airport Master Plan.

Most airports with international flights have a Federal Inspection Service (FIS) SSCP. This is a checkpoint where arriving international passengers are required to be screened before transferring to a domestic flight. The reason is that the U.S. screening process has different requirements and provisions than screening processes in many international airports in other countries where a passenger may have originated. The screening requirements for a FIS checkpoint are the same as other U.S. checkpoints but the volume varies based on the frequency of inbound international flights.

e. Elements of the SSCP

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

1) Pre-screening Preparation Zone

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

2) Queuing Space

The queue is where passengers stand in line at the front of the checkpoint on the public side. It is recommended that the queue be bounded by double strap stanchions along the perimeter with single strap stanchions defining the various lanes from the queue entrance(s) to the TDC(s). Queue lanes are approximately 3'-0" to 5'-0" wide depending on the lane function and queue space available.

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

SSCP layout can affect the queue dramatically. When evaluating queuing space, consult with local TSA on the current wait time standard as well as reviewing the results of the analysis conducted for Capacity, Arrival Distribution, and Section 1d of the SSCP Rates & Standards. TSA also suggests estimating a minimum of 9 square feet per passenger.

3) Travel Document Checker (TDC)

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

a) The TDC should be setup so that NO individual can circumvent or bypass the TDC podium.

b) The TDC podium should be approximately 6'0" to 10'0" from the divest end of each lane in order to allow passengers to move freely toward their chosen lane

c) Create alternating “mini-queues” on both sides of the TDC podium by providing stanchions in front of the podium. This will force the passengers to form two separate lines for the same TDC. The TDC will process whichever “mini-queue” passenger is ready (refer to *Figure III-F-4*).

4) Carry-On Baggage X-Ray Machine

Carry-on bag screening is mandatory at a SSCP. This screening process is accomplished by X-ray machines of various types and manufacturers. This equipment generally has the following similar components:

a) Loading Table/Entrance Roller Conveyor;

b) In-feed Tunnel;

c) Scanning Belt (continuous from In-feed to Out-feed Tunnel);

d) X-ray Dome;

e) Out-feed Tunnel including alarm bag cut-out;

f) High Speed Conveyor (HSC) & Tunnel; and

g) Extension Rollers and/or Exit Roller.

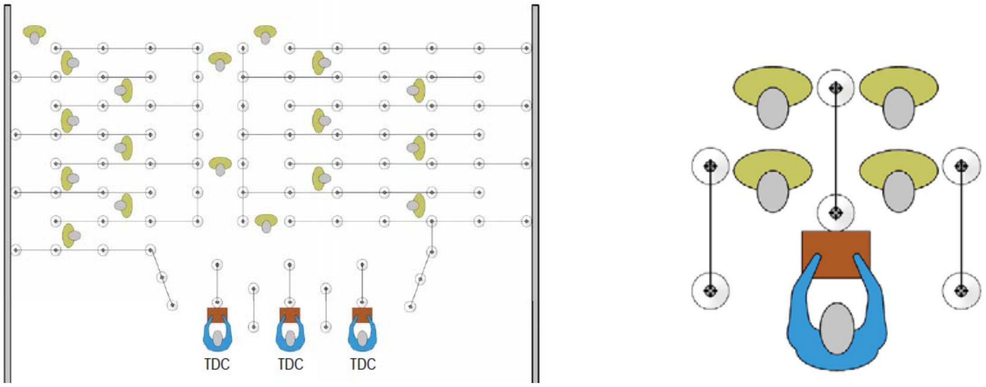


Figure III-F-2—TDC with Alternating "Mini-Queues"

Interpreting the bag images on the monitor requires focused concentration by the TSO. The operator should have an ergonomic and distraction-free environment. The space should be designed to minimize glare on the monitor from interior lighting, glass walls, or sunlight. The monitor height should be at an optimal viewing angle. The operator must also have a clear view of the machine's entrance and exit conveyor. Columns, power poles, and signage, etc., should not prevent the TSO from seeing the bags going in and the bags going out of the X-ray unit.

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

5) Walk Through Metal Detector (WTMD)

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

6) Barriers (F) & ADA Gates (G)

In order to prevent passengers and/or items from passing into the sterile area from the non-sterile area without being screened, barriers and/or ADA gates should be installed to close all gaps exceeding 12" across the front width or façade of the checkpoint.

The ADA gate is part of the line that separates the non-sterile area from the sterile area. However, the ADA gate allows passengers to reach the sterile area that cannot otherwise traverse the WTMD.

7) Advanced Imaging Technology (AIT)

The implementation and operation of AIT systems as the primary screening method maximizes the likelihood that TSOs will detect potential threats while preserving passengers' privacy. At the time of this publication, the use of AIT is a major paradigm shift away from metallic based threat detection toward organic threats placed on the body. Incorporation of this and other evolving technologies into the checkpoint environment is part of a layered approach to the dynamic SSCP Standard Operating Procedures (SOP) for primary passenger screening.

8) Holding Stations

A holding station holds passengers temporarily until screeners are available to escort them to the proper area to conduct secondary screening. The holding station should be positioned so passengers can be diverted directly into the area without obstructing the path of non-alarming passengers, and should prevent the passing of prohibited items to sterile passengers.

9) Explosives Trace Detection (ETD), Bottle Liquid Scanner (BLS), Alternate Viewing Station (AVS)

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

10) Private Search Area

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

11) Egress Seating Area

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

12) Supervisory Transportation Security Officer (STSO) Podium

The STSO should be able to perform administrative duties while periodically viewing the entire screening operation with minimal obstructions. The STSO should be located on the sterile side near the checkpoint exit to allow for adequate viewing of the overall operation.

13) Exit Lane

An exit lane is often co-located adjacent to a checkpoint or it can be located independent of the checkpoint. This lane should be easily identifiable without adversely affecting security and adequately sized for deplaning passengers exiting the concourse. All building code egress path requirements must be met.

14) SSCP Adjacent Walls & Boundaries

There is no set boundary for an SSCP. It will vary by airport, SSCP configuration, and TSA requirements and throughput estimates for a particular checkpoint. The SSCP length starts at the TDC podium(s), extends through the checkpoint elements discussed in this section, and ends at the checkpoint exit, which could be adjacent to the egress seating area, STSO or LEO podium. The SSCP width is the wall to wall width of the checkpoint, including all the screening lanes and any collocated exit lane. All walls adjacent to the non-sterile side need to be at least 8'0" high to prevent the passage of prohibited items from the non-sterile area to the sterile area. In the future, new technology may extend the boundaries of the SSCP to include additional equipment and functions within the checkpoint or equipment and functions located remotely within the airport.

f. SSCP Power & Data

The power and IT requirements for security screening equipment and ancillary equipment for piece of equipment is unique in regard to the circuit type, receptacle type and quantity of data drops required. Location of the electrical and data outlets in reference to the equipment is also critical. Familiarity with these requirements will be essential when designing a new checkpoint or reconfiguring an existing checkpoint. For detailed specifications and requirements, please refer to the most recent version of the TSA Checkpoint Design Guide Standard, as well as Part III, Section I of this Guidelines document on IT and power requirements.

1) Equipment Requirements, Receptacles and Locations

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

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

In some cases a new electrical panel may be required for new circuits in support of a new checkpoint or reconfiguration of an existing checkpoint. This requirement will be determined during the design phase by an electrical engineer. The electrical design of a new checkpoint or reconfiguration of an existing checkpoint must meet national and local codes in addition to any airport, State, county, and/or city requirements, depending on the Authority Having Jurisdiction. Uninterrupted power supply (UPS) backup power is not required for SSCPs, although it may exist or be required at some sites. Power and data receptacles should be of high quality industrial standard to accommodate high volume traffic through a SSCP. All power/data poke-through devices (flush or recessed), pedestals/monuments (surface mounted boxes, i.e., “tombstone”), power poles, fittings, and/or plates must be coordinated with the airport operator and the TSA. Power and data receptacles should be of high quality industrial standard to accommodate high volume traffic through a SSCP.

In addition to receptacle type and finish, the airport should approve core drill sizes and locations of electrical trenches. Poke-through and pedestal receptacles should be positioned in such a way as to avoid trip hazards for both passengers and TSA personnel. Extension cords for permanently installed equipment are unacceptable if the equipment cord is too short to reach a receptacle. The most preferred method of running electrical and data is in a Walker duct/trench system as illustrated in *Figure III-F-5.*

a) Benefits

- Large capacity for routing wiring and cables beneath floors.
- Cost savings for drilling and X-ray of floors every time a core drill is needed or relocated.
- Provides easy access to wiring and cabling in the floor with removable panels or access though the raceway.
- Flexible construction using modular components to create a floor duct system or raceway.

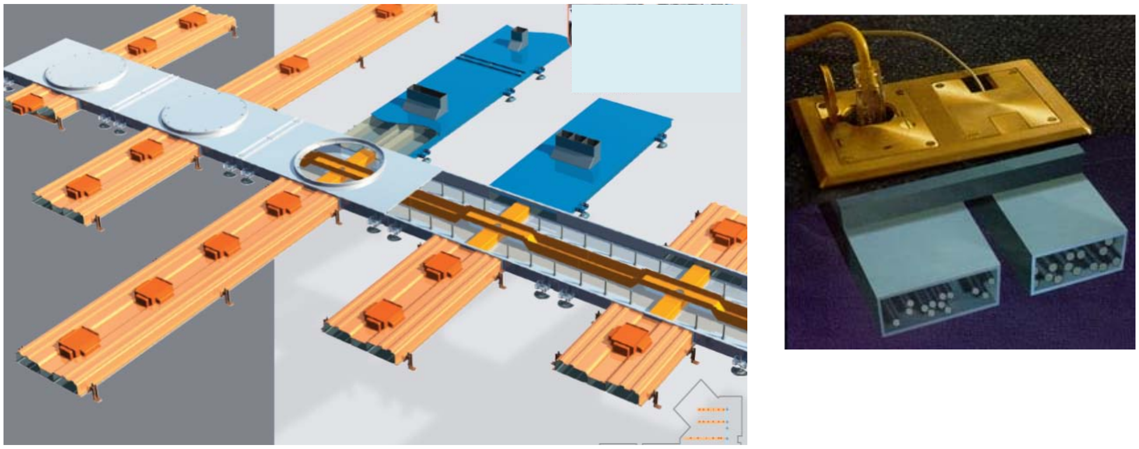


Figure III-F-3—Example of Power & Data Under-Floor Distribution

- Future needs met without disturbing floor by relocating/adding/removing components.
- Use separate compartments per electrical code and specific needs—i.e., separation of power and data wiring.
- Typically comes in four (4) widths—6", 12", 18", and 24"
- Typically comes in two (2) depths—2-1/2" and 3-1/4"
- Load capacities as follows:
  - 6" width no supports—up to 2400 lbs concentrated load;
  - 12" width no supports—up to 2400 lbs concentrated load;
  - 18" width one support row—up to 2000 lbs concentrated load; and
  - 24" width one support row—up to 2000 lbs concentrated load.

b) Installation Considerations

- Requires cutting a floor trench to install in an existing concrete floor slab—for use in new construction.
- Requires coordination of the installation with structural components in a floor slab such as reinforcing rods, steel, existing in-floor devices, and conduits, etc.
- Refer to specific vendor cut sheets for additional details.

2) SSCP Lighting

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

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

3) Closed Circuit Television (CCTV)

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

g. Safety

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

h. 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 for the SSCP.

i. Designing for the Future

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 should be sufficiently adaptable to meet the changing threats and support the equipment that detects these threats. Security screening equipment dimensions and/or processes may change, requiring the entire airport security managerial infrastructure to make important decisions regarding modifications, which the designer must then accommodate. The designer's task will be easier if the original design has anticipated the need for change and allowed for size and space adjustments by surrounding the SSCP with as much flexibility and potential expansion space as possible.

Section III-F-1—Security Screening Checkpoints (SSCP) Design Checklist:

□ **Refer to Primary TSA Guidance Document**

□ **TSA, airport and airline should be consulted**

□ **Planning Considerations**

- Level and type of risk
- Airport operational type
- Location of SSCP

□ **Elements of the SSCP**

- A—Prescreening preparation zone
- B—Queuing space
- C—Travel document checker
- D—Carry-on X-ray
- E—Walk through metal detector
- F—Non-metallic barriers
- G—Non-metallic ADA gate/access
- H—AIT machine
- I—Holding stations
- J—Trace detection
- K—Private search area
- L—Egress seating area
- M—Supervisor station
- N—Exit travel lane
- O—Checkpoint boundaries

□ **SSCP Signage**

□ **Space for TSA Staff**

□ **SSCP Layout and spacing standards**

□ **Designing for the Future**

Section G—Access Control

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

Note that airport access control systems are not designed to control the access of passengers and specifically not for a "Trusted" or "Registered" traveler program. Access control systems are normally considered in two parts: the first provides the vetting, approval and credential issuance process, and the second is a physical access control system that uses the resulting credential to provide or deny access.

1. Credentialing

   a. Credentialing is the process by which an individual is issued a credential that visually (and in some cases electronically) identifies the person as having been granted privileges for unescorted access to secure and sterile areas on an airport. The credential is normally in the form of a conventional ID badge often called a SIDA (Security Identification Display Area) badge.

      The credentialing process has several major sub-processes:

      1) Determining an applicant's identity through scrutiny of an applicant's official identity documents (known as "breeder documents");

      2) Verifying the applicant's identity and biometric information by a regulatory clearance process to determine if that individual is qualified to have an airport ID badge and related access privileges;

      3) Collecting the individual's ten fingerprint images and biographical data for conducting a Criminal History Records Check (CHRC) and a Security Threat Assessment (STA) that checks against a number of Federal data bases by using the facilities of an aviation channeling service provider (i.e., a fee-based authorized entity that provides and facilitates the exchange of fingerprint images and biographical data to/from the airport and TSA for background screening purposes);

      4) Submitting fingerprint and biographic data for conducting a check against State or local data bases (only required for some locations);

      5) Conducting airport specific security training of the applicant; and

      6) Issuing a credential along with appropriate access privileges for that facility.

      There are a number of different mechanisms or models to implement these functions. More details are provided in the RTCA DO-230C document.

      It should be noted that while an applicant's biometrics (currently fingerprints of all ten fingers) must be submitted to Federal authorities for checks against criminal records in order to obtain the required clearances, a biometric of any type (apart from a facial image on a badge) is not currently required by Federal regulations for use with a physical access control system at airports. However, some airports have chosen to deploy such systems.

      There is also a need for an adjudication process in the event of a negative determination at any stage, and there are significant record keeping and audit requirements, which are subject to TSA inspection

   b. Under the current (2011) TSA regulations, the credentialing process must be performed by each airport operator regardless of what privileges or similar credentials an applicant may have at another airport. This is for two reasons:

      1) Some states have additional regulatory requirements which effectively means the collection and submission of fingerprint records to local authorities for background screening has to be repeated regardless of previous clearances by Federal authorities.

      2) There is (as yet) no standard credential, backed up by an appropriate issuance, management and repudiation process which allows individuals to establish their Federal regulatory clearance status for use by any other airport.

Note that even with such a standard credential, each individual would still have to be approved by an authorized entity at each airport (normally, but not always, the airport operator) to obtain an airport-specific credential. In addition, each airport has a mandatory airport security training program that each individual must complete before being issued an airport credential. The type of training typically depends on the nature and scope of access permitted, including special training for persons with ramp driving privileges.

c. Thus, there are effectively two types of credentials:

1) an identity credential (typically an ID badge) used to verify the individual's identity (and potentially to verify Federal clearances in the future); and

2) an access credential (typically a badge or a fob), or a combination with the ID badge, by which the access control system will allow entry to secure areas at that specific airport.

These credentials need not be the same, but are currently most often incorporated into a single unit for accountability and user convenience

d. Credentialing Interoperability

The concept of an interoperable credential has emerged which would make it unnecessary for individuals with the requirement to work at more than one airport to be separately processed for each airport where they may work. It is likely that any such interoperable credential would be used primarily for the purpose of establishing identity and not for access control purposes.

Since the last guidelines were issued, a new proposed mechanism has evolved for an interoperable credential that would be used by first responders and mutual aid personnel. The concept is called First Responder Authentication Credential (FRAC). While not a Federal requirement, airports should carefully consider if they need to support such a program which allows the verification of the identity and qualifications of off-airport first responders and mutual aid staff in an incident or an emergency.

Alternatives for accepting such credentials include providing a central point at which credential authentication can be performed or using hand-held battery powered devices for this function. The decision whether or not to support interoperable credentials, and the sophistication of implementation, is up to the individual airport.

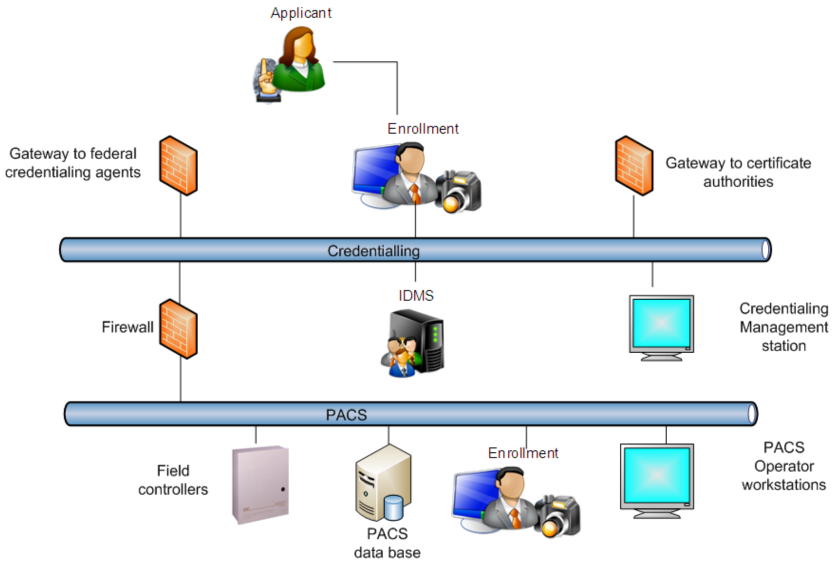

Applicant
Enrollment
Gateway to federal credentialing agents
Gateway to certificate authorities
Credentialling
IDMS
Firewall
Credentialing Management station
PACS
Field controllers
PACS data base
Enrollment
PACS Operator workstations

Figure III-G-1

Credentialing System Components (Simplified)

2. Physical Access Control

This is the part of the system which allows or denies entry to secure and/or sterile areas of the airport on the basis of a credential issued by the credentialing process. Such systems usually involve a computerized system of credential readers, (normally but not always badge readers), automatic door locks, and perimeter portals located throughout an airport by which only individuals with an airport issued or airport approved credential embedded with appropriate permissions can pass through access portals, and enter secure and sterile areas. However, at smaller airports, physical access control could also be based on simple lock and key methods and/or physical guards.

Note that this represents an entirely separate function from identification, although access information is often carried on the same media. In the past, these two processes were typically implemented in a single system with a standalone fingerprint unit for collecting the ten fingerprints required for the background screening process. However, increases in regulatory requirements have led in many cases to there being two separate systems.

The definition and topology of each airport's secured and sterile areas is airport specific, but is based on the regulatory requirements in 49 CFR §1542. Larger airports can have hundreds of such portals monitored by such devices; smaller airports may have only a handful.

The cost and installation effort and duration for these systems and their supporting infrastructure is significant, and much of the currently installed local control equipment is proprietary. This effectively means that once a specific manufacturer's system is established at an airport, any new entry portals will need systems compatible with that manufacturer's equipment.

Access credentials can be of several types. Previously most airport access credentials were simple magnetic stripe cards. Most modern systems now use various forms of contactless card technologies, the credential being either a conventional proximity card or a high frequency transmission smart card. Typically such access control systems do not just accept a credential for access; they can use another "factor" to establish authority before permitting access at a portal. Normally this is a PIN, a concept familiar through its common use with banking ATM cards. In some limited circumstances, compatible credentials might also be issued by an airport-approved third party such as an airline or tenant, but typically they would be valid for use only in very limited parts of the airport such as a carrier's exclusive use areas.

Most airport installations do not yet use "biometrics" (e.g., fingerprints, face, hand, iris, vein, etc.) at access control portals as an additional factor to verify the identity of the person requesting access. However, this higher degree of security may be warranted for some strategically significant facilities, or high risk entry portals, even if biometrics are not currently a Federal requirement.

Detailed standards and guidelines for Physical Access Control credentials are provided in the RTCA DO-230C "Integrated Security System Standard for Airport Access Control."

a. Regulatory Requirements Overview

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

Such directives can be obtained on a "need to know" basis only from the Federal Security Director associated with each airport . These directives specify requirements for both the credentialing process and the physical access system.

An airport's access control systems and procedures are detailed, from an operational perspective, in each airport's Federally mandated Airport Security Program (ASP). These programs are designated Sensitive Security Information (SSI) and are also only shared on a "need to know" basis in accordance with 49 CFR 1520.

Note that airports exclusively serving General Aviation (GA) are not currently required by regulation to have such access control systems, although this is considered an industry best practice. Security Guidelines for General Aviation Airports are available from TSA and address some possible GA applications for access control.

General aviation facilities at regulated airports must also comply with the airport's overall requirements in the airport's ASP.

b. Operational Requirements

Airport staff access control systems have four main operational requirements:

1) to issue access credentials in line with TSA and other regulatory requirements;

2) to monitor access to the secure and sterile areas using these credentials;

3) to annunciate any security violations, and access to areas without an appropriate credential; and

4) to record and log all pertinent events, and provide reports as necessary.

Normally at all but the smallest airports, this is achieved by an electronic access control system.

1) Issuing credentials

   The airport is responsible for issuing credentials and for their on-going management in accordance with TSA regulations. Normally a credential is either a conventional plain ID badge or a badge with some form of internal electronic coding or a smart card.

2) Monitoring

   The primary purpose of an access control system is to deny access to unauthorized persons, and to control access by authorized staff to specified secure and sterile areas. This is often done by means of an ID/access combination credential presented to an electronic card reader at a portal, or other entry point to a secure area. Other infrequently used entry points, such as roof hatches may be secured using conventional means, e.g., padlocks and/or alarm sensors.

   The system verifies whether the owner of the credential 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. PIN or biometrics can be used as additional authentication factors.

   Many airports also use such access systems to control access to AOA and other areas not designated as secure areas, as well as to airport administrative areas not located in secured areas. This is not a regulatory requirement but is common practice.

3) 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 some form of denial of access.

   This annunciation can be accomplished locally by means of a local alarm at the door, and remotely at a “dispatch” or control center monitoring the alarms and capable of dispatching appropriate response personnel to the scene of the denial or breach.

4) Recording of events

   This function is to record and automatically log all attempts to enter secure and sterile areas, whether successful or unsuccessful, and to provide reports as required. Such data should be kept for a period of at least 12 months, or as defined in the ASP.

5) 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 found in the RTCA DO-230C document referenced above.

6) Selectivity

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

   These are Sterile, Secured, SIDA and AOA (See *Figure II-C-1* in Section A) areas that correspond respectively to security measures for interior terminal areas past screening checkpoints (sterile), exterior airside areas where aircraft are docked or parked (secure), airside areas requiring security identification display (SIDA), and the airfield itself which includes runways and taxiways (AOA), as well as terminal and cargo ramp areas, which may include more than one such area.

   Cargo areas are also included, depending upon their location within the security related areas. (Cargo is addressed at greater length in Part III, Section D.)

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

c. Typical Physical Access Control System Components

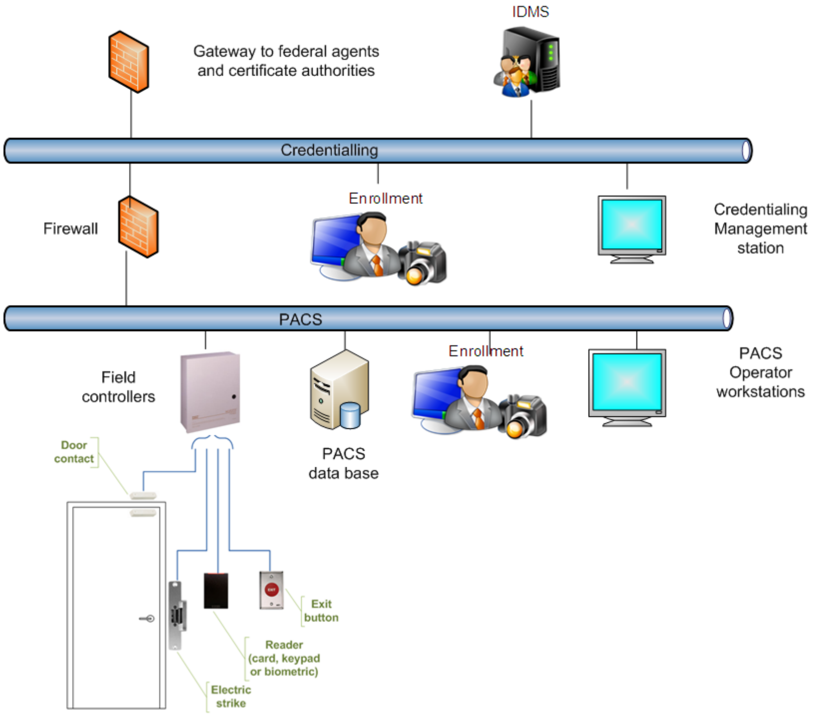

IDMS
Gateway to federal agents and certificate authorities
Credentialling
Firewall
Enrollment
Credentialing Management station
PACS
Field controllers
Enrollment
PACS Operator workstations
PACS data base
Door contact
Exit button
Reader (card, keypad or biometric)
Electric strike

Figure III-G-2

Physical Access Control System Components (Simplified)

1) General

A physical access control system typically consists of three main components:

a) portal hardware;

b) field controllers; and

c) central servers.

Portal hardware includes card/badge readers and portal locking/unlocking hardware mechanisms and switches. These are conventional components common with almost any physical access control system used in many applications. Many portal hardware devices are system manufacturer independent.

The field controllers (or field panels) are typically microprocessors and panels that control and can manage several portals and field devices. Typically, these devices contain a partial database of local cardholder and privilege information, and provide a degree of stand-alone operation should any communication links to the central server(s) be lost. These units are normally supplier specific and cannot easily be mixed with another supplier.

The central server(s) provide the access control system primary database and is used to perform administrative and transaction recording (logging) functions and other central functions.

These server(s) are typically based on conventional operating system platforms and hardware technology with supplier-specific application software.

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

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

Details of each of these components and recommendations are provided in the RTCA DO-230C standard.

2) Biometric Readers

Some airports have decided to utilize biometrics as an additional method of user authentication in their physical access control systems. This means that within the selected portal reader(s), in addition to having a conventional badge or credential reader, a biometric sensor device and associated software algorithms are also available to collect and compare the biometric characteristics of the person who is using the credential with the biometrics previously enrolled at badge or credential issuance.

The biometric technology used for physical access need not be the same technology as that utilized for background screening purposes and may be airport specific.

The majority of airports using biometrics have chosen to implement fingerprint technology since fingerprint is the most mature and tested biometric with the widest choice of vendors, competitive prices and an array of published standards. A discussion of the types of biometrics, how they operate and the choice options are outlined in the RTCA DO-230C standard.

Note that it is not necessary that all access portal readers have a biometric capability. Biometrics could be incorporated in readers for only in those entry portals determined to be high risk on a threat-based analysis, or might be activated only during elevated risk conditions. As a result, some airports may deploy only a small number of biometric-enabled readers while others may deploy such readers more widely.

The biometric matching function typically takes place in the portal reader device. This method is known as “match-on-reader” where the previously enrolled biometric data is read from the credential and the matching function takes place within the reader. This approach eliminates the need to maintain a local database of biometric templates and the time delay and cost associated with sending the presented biometric template to a central server for matching. However, there should be protections against unauthorized tampering with the reader device at the entry portal such that the reader cannot be altered to always return a result indicating a positive biometric match. Cryptographic mechanisms should be employed to ensure the validity of the biometric that is read from the credential.

It is also possible to perform the biometric match comparison inside the logic of the smart card integrated circuit chip itself. This approach is commonly referred to as “match-on-card.” If the match is successful, the user-unique ID number is read from the card and sent to the field controller panel. Cryptographic mechanisms should also be employed to transfer trust in the biometric match result between the credential and the reader. The field controller panel will make the decision to grant / deny access based on authorization privileges granted to that user. Refer to RTCA DO-230C for more details.

3) Personal Identity Verification (PIV) Readers

Portal reader (and hand held portable) devices that are now commercially available are designed to function with interoperable smart cards based on the Federal Information Processing Standard (FIPS) 201 for Personal Identity Verification (PIV) of Federal workers and contractors. If the decision is to utilize a PIV-type credential, with or without a biometric, additional system and operational requirements may ensue.

These requirements are a consequence of the PIV technology and standards. Essentially, the reader will need to read and process the various data objects on the PIV card according to the technical specifications associated with the FIPS 201 standard.

This could include the ability to read and process the credential holder's digital certificates encoded on such cards, and also to potentially have access to a Public Key Infrastructure (PKI) to check the validity of the certificates and confirm that the certificates have not been revoked by the issuing authority.

Depending on how such a system is implemented, this could require an Internet Protocol (IP) connection to each portal reader. An alternative could be to perform periodic certificate validation for those registered card holders through the central server during idle time or in background mode.

Implementation of PIV-type credentials and readers can be complex in a PACS environment. For technical details, see the RTCA DO-230C standard and the National Institute of Standards and Technology (NIST) publications related to PIV.

4) Mobile Credential Readers

An increasing number of airports are deploying mobile credential readers. These allow on-the-spot verification of an individual's airport credential, independent of the network of fixed badge and credential readers around the airport.

This has proved to be an effective security system supplement. These readers can electronically verify the credential and can also hold a biometric of the person to whom each credential was issued to add a further level of verification.

Several options are possible: it could be as simple as display of a facial image stored on a smart card for visual comparison with the person, or it could include performing verification of a biometric taken during enrollment, which could be read off the card, even if the fixed credential readers do not support this functionality.

d. Support Requirements

Access control systems at airports have three major support requirements:

- power;
- communications; and
- HVAC.

The current RTCA standard DO-230C identifies specific requirements in some detail. A summary is given below.

1) Power Requirements

In general, access control systems have three power requirements:

- at the central server(s);
- at the field controller; and
- at the portal or reader device.

Each requires power to operate. This power should be provided via a UPS (normally using batteries), which should be connected to backed-up power to ensure continuous operation even during an extended power failure.

Electrical power integrity for security systems is vital. Backup and standby power should be designed to ensure that security functions will continue to operate at the level of service required by the TSA. The metric for cutover to backup power in security systems is a maximum of 50 msec, if not provided by a UPS. This metric should apply unless the TSA has specified an alternative requirement. Electrical power for any system component, whether running on the terminal's electrical grid or on a separate primary power source, should be reviewed to ensure that the design provides the required backup and standby level of service.

Failures and significant events affecting power should be enunciated at the airport security operating center (SOC) even if there is a separate monitoring capability available.

a) Central Servers

Servers are usually located in a main equipment room which typically has both backed-up and UPS power available. Access control system servers and communication controllers do not typically require large amounts of power, but their requirements need to be factored into the total power requirements. A UPS for a processor should provide at least four hours of system service after main power failure. (Refer to Part III, Section I, IT-Power.)

b) Field Controller

Field controllers (also called field panels) are usually located in communication closets which should be placed typically in secured areas and only accessible to authorized personnel. If they cannot be so located, then they should be located in a hard-to-reach area or one which is under continuous surveillance.

Most field controllers run on their own local power supply with a built-in UPS. The load is seldom large. A UPS for a field controller or panel should provide at least four hours of system service after main power failure. Sometimes these are integrated with the controller.

c) Device Power Requirements

There are two types of door and portal devices are of two types: those that require little power, such as door sensors and credential readers, and those that require more power such as magnetic locks.

Depending on the system manufacturer, the power, if required, to such low power devices, (typically but not always 24VDC), is either generated locally from a backed-up supply or centrally at the nearest closet via a UPS. (Refer to Part III, Section I—IT-Power.)

Magnetic locks have a more significant power draw and provision of a UPS capability of any reasonable time duration is a design issue, but at least 20 minutes should be provided. Note that there may be some fire code regulations on the use of magnetic locks on some doors.

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, (though which many are not). Otherwise, conventional low voltage wiring from the communication closet can be deployed. These devices should have at least four hours of UPS available.

Some access system devices will be located on the perimeter or other remote locations (refer to Part III, Section A), and these sometimes bring special power challenges, such as use of solar power. Each location should be assessed according to its own circumstances. Note that this subject is covered in detail in the RTCA DO-230C standard.

2) Communications Requirements

In general, on-site communication requirements of physical access control systems at airports have three components:

- The requirement to link the devices at portals to field controller panels (secondary or horizontal wiring);
- The requirement to link these field controller devices back to a central server (vertical, backbone or primary wiring); and
- The requirement to link back to any regulatory agencies or credential clearing services.

This subject is covered in detail in the RTCA DO-230C standard.

a) On-airport Backbone Infrastructure

This provides capability to link local control panels back to central servers, and monitoring consoles back to central servers in a similar way.

Current access controls systems, with the exception of the smallest, use a standard IP-based backbone communication structure. As such, new systems could easily share a common physical communication infrastructure (see Part III, Section I, IT-Power) for communicating between the main server, which typically holds the access control data base, and the panels and monitoring stations.

b) Secondary Infrastructure

Current access control 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 rapidly coming onto the marketplace, and could share a common infrastructure if such was extended to the secondary distribution. Note that not many facilities have such a common secondary infrastructure. If one is not available, the appropriate wiring is the responsibility of the access system supplier.

c) Off-airport Communications

Until recently, airport access control systems were a closed system (i.e., one without any connection to the outside world and specifically not to the Internet). However, the requirement to interface a credentialing system to central security clearance service providers and/or Federal agencies has led to a requirement to provide such systems with a suitable link.

At one time, these links were only connected to stand-alone fingerprint live-scan systems used for applicant screening purposes. Such systems had a direct communication link to the agency or service provider. However, at larger airports these are now directly connected to the credential management or badging system to eliminate the requirement for redundant data entry. In addition, with the series of Security Directives over recent years regarding Security Threat Assessments (STA), a variety of communication link options have been deployed.

These systems are still in a transition state at time of this publication. Eventually these are expected to migrate towards a standardized virtual private network (VPN) structure over conventional Internet connectivity services.

Normally these systems are completely separate from the badging systems. In the future, a secure controlled link between the two, to enable the passing of data and thus avoid the need for re-entry of data will probably be standard. Some larger airports have already implemented such a link.

Finally, it is important to note an increasing worldwide prevalence of sophisticated cyber attacks on government and other secure facilities. Each airport should consider this in all its links to external systems, not just in security systems, but in all shared communication links with conventional airport information technology (IT) systems, and other Federal and State agency systems.

d) Use of Onsite Shared Communications Infrastructure

The current RTCA DO-230C standard provides specific technical guidance related to shared communications. This guidance includes details on how the use of a common infrastructure should be deployed to maintain a high level of security appropriate for access control and alarm monitoring systems. Essentially, this allows the use of shared physical communications infrastructure but requires physical separation of control of the fiber and copper for security systems.

e) Use of Onsite Common and Shared Networks

The current RTCA standard specifically recommends against the use of shared networks for access control systems with few special exceptions. 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. A common issue here is that while conventional IT systems require frequent upgrades, access control systems are typically much less frequently updated. This can lead to issues of incompatibility. Further, conventional IT systems frequently require reconfiguration; while access control systems do not have the same profile.

It is generally true that with the increased complexity comes an increased risk of operator error. Each airport operator needs to carefully examine the local circumstances and advantages of using a common network.

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

Point-to-point 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 efficiently in all weather circumstances.

g) Maintenance Considerations

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

h) Perimeter Devices

Note that some access system devices will be located on the perimeter or other relatively remote locations and these sometime provide special communication challenges. Each location should be assessed according to its own circumstances.

i) Monitoring

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

j) HVAC Requirements

These requirements are often overlooked. Some communication switches and servers can generate significant amounts of heat. While card readers and field panels are usually moderate in their requirements, the heat from switches can adversely impact an installation's environment.

The impact of any new equipment's heat generation should be identified as well as the existing HVAC capabilities of any room or closet in which they are located. Conversely, in very cold environments, the effect of the cold conditions should be determined on all components, particularly those located on the exterior of facilities.

3) Special Device Considerations

a) Anti-tailgating Devices

The purpose of anti-tailgating devices is to stop people and vehicles from tailgating through an entry portal. Vehicle anti-tailgating measures are covered in Airport Layout and Boundaries. Personnel anti-tailgating devices are of two types:

- anti-tailgating devices, such as turnstiles specially manufactured for that purpose; and
- additional general-purpose sensors/devices attached to the existing portal.

Devices are typically interfaced to an access control 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 event. Systems based on video analysis may need operator interpretation.

b) ADA Issues

A subset of the access portals is that airports are required to be compliant with the Americans with Disabilities Act of 1990 (ADA). This requires additional equipment and additional clearances at the portals. In addition, some states and cities have additional requirements over and above those specified in the Federal 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 can make this difficult to avoid and still remain within local fire codes. Included in these measures are crash bars linked to the access control system to detect unauthorized operation of these doors.

This is especially important on fire doors that give access from public or sterile areas directly to secure areas and the Aircraft Operations Area (AOA). For non-emergency use, the doors are usually equipped with credential or badge readers that can be used to deactivate the alarm (See Part III, Section D, Terminal for further discussion of fire doors and emergency exits).

d) Elevators

Elevators should not allow access from public to secure areas. However, some unique circumstances may not always make this possible, and dual use elevators are not uncommon. In the event of dual use, the controls to access the secured and sterile areas need to be under the control of the access control system wherever practical.

In addition, airport operators should consider occupancy detection, and internal video surveillance, so that an elevator cannot be boarded at a public floor and then brought down to a secure floor with a passenger without warning or positive controls.

e) Environmental Requirements

Use of access control systems inside facilities presents minimal environmental challenges. However, systems deployed in outside or exposed baggage handling areas with dirt, dust, heat or snow presents some challenges to the electronics and the actual operation. The RTCA standard DO-230C standard covers these requirements.

f) Legacy System Integration

Except in some completely green-field sites, there will almost certainly be some form of legacy system which may need to be interfaced to a new physical access control system. Interfacing of such systems can be complex and is covered in the RTCA DO-230C standard. Generally, however, the simpler the interface the better.

4) Integration with Other Systems

Security systems with which access control system integration is typically required include CCTV, perimeter surveillance and sensors, duress alarms, and others identified below.

a) CCTV

Closed-circuit television (CCTV) is widely used in association with access control systems in order to effectively monitor an access portal. Details of video surveillance requirements are given in Video Surveillance in Part III, Section H. From an access control system point of view, there are three main requirements:

i) The CCTV cameras should be located to provide as good a view as possible of the portal, so that the full portal area can be monitored effectively. Selection of each location and camera type depends on operational mode and local topology (i.e., viewing on both sides, or one side of a portal).

ii) The CCTV system should be linked with the access control system such that when an alarm or other identified event occurs, the video from the CCTV camera(s) is automatically switched on and the video presented at the appropriate monitoring location, typically a security operating center or SOC.

iii) 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 facilitate later 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 and resolution for this clip. The duration of this clip should be configurable per portal.

Issues related to the sharing and release of video imagery taken by security cameras are addressed in the Video Surveillance section of this document and also in the RTCA DO-230C standard.

Much security event data may 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 Plan (ASP).

b) Perimeter Intrusion Detection Systems (PIDS)

Perimeter intrusion detection systems are designed to monitor and detect vehicles and personnel crossing the airport perimeter. These can be monitored by a separate system but most airports have chosen to link these into a single system for convenience. Numerous perimeter intrusion technologies are available, particularly for other facilities such a fuel farms and cargo areas which use similar technologies. See Part III, Section H for further details.

c) Duress Alarms

Duress alarms can be installed at various locations throughout an airport. This includes checkpoints, but could also include dispatch offices, Customs and Border Protection (CBP), and even the check-in and ticket counters. Location and installation of these devices is airport and operational model dependent. These devices are usually linked back into an access control system to provide a common annunciation point for operational effectiveness and convenience, but could also be linked back to a CCTV system.

d) Vehicle Gates

Vehicle gates are described in Part III, Section A on Airport Layout and Boundaries. Due to the regulatory requirements and Security Directives associated with security gates, there is a clear requirement to link these back to the airport access control system to provide the same level of control and response as at standard portals.

e) EDS, EOD and ETD Support

Some airports have chosen to install access control devices in EDS, EOD and ETD areas so as to secure the areas and prevent theft and interference with equipment. This decision should be based on local conditions and operational practices.

f) Checkpoint Issues

Passenger screening checkpoints present some unique challenges for access control. These are in four areas.

i) First is the need to secure the checkpoint and the access route via the checkpoint when it is not in use. This requires locking doors or rollup mesh screens. The checkpoint may be locked from one side or both depending on the airport configuration. Such doors should be controlled and monitored by the airport access control system.

ii) Second, there is the growing requirement to validate credentials of Federal Air Marshals (FAMs), law enforcement officers (LEOs) and pilots who bypass the screening position because they are carrying weapons. There is also a growing interest in implementing a secure process for alternate access for certain flight deck and cabin crew members in lieu of the conventional passenger screening process. At present, there is no centralized system for such credentials, but this is likely to change during the life cycle of this document.

iii) Third is the issue of the exit lane. At some airports this is co-located with the checkpoint; at others it is separate. In either case, this exit lane should have access control or some alternative form of counter flow control. At some airports, there have been attempts to automate the detection of any counter flows in this exit route so that staffed operations are not required. At least two such studies are underway as this document was in preparation. Note that where the exit lane is collocated, the current standard practice is for the TSA to staff the location.

iv) Finally, there is potential for an application at a passenger screening checkpoint that in the event of a breakthrough or other breach, that the associated concourse and other portals can be promptly secured to reduce the impact on operations and assist in returning the concourse to normal operations. The ability to effectively achieve this depends on the concourse's topology and local fire codes.

g) Integration Risk Reduction

Integration among systems has proven to be one of the most problem-prone areas of airport security from a technical point of view. Some of these problems have been caused by an over-enthusiasm with vendor claims for new technology and an underestimation of related implementation and installation issues. Where possible, pre-procurement testing in the proposed airport environment can be quite helpful in evaluating and verifying vendor claims.

e. Federal Inspection Services (FIS) Device Requirements

1) Special Security Requirements

FIS Areas, primarily Customs and Border Protection (CBP), are another category of security area. The requirements for security and the delineation of these areas is described to some degree in Appendix F of this document, and found in detail in the CBP Airport Technical Design Standards. CBP approvals are obtained through the CBP Office of Internal Affairs.

2) 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, which typically varies depending on size and space requirements. CBP approvals are obtained through the CBP Office of Internal Affairs.

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

f. Command and Control Requirements

For technical requirements on integration for command and control see Part IV Appendix E and the RTCA DO-230C document.

1) Security Operations Center

An access system must be monitored at some location so that appropriate responses to alarms can be made, and staff and resources dispatched accordingly. There is typically a command and control center of some type, often called an SOC, or Security Operations Center. This center can be located either in the facility being monitored, or often at a centralized location for an entire airport. Not just access control, but CCTV and other security systems are often monitored at these locations.

See Part III, Section D - Terminal for further discussion of this issue.

2) Badging or Credentialing Center

Each airport needs a location at which airport-specific credentials are issued, (and potentially interoperable credentials in the future). For small airports, the requirements are typically modest. For larger airports, the space required is so large that to include it in a terminal is often not practical; there are continuing issuance and re-issuance requirements even for existing staff.

The minimum enrollment center requires a workstation, a badge/card printer, and a fingerprint or live scan collection device. Larger airports may need multiple workstations, multiple fingerprint devices and multiple badge printers; and perhaps a "Department of Motor Vehicles" type layout to serve multiple queues of applicants.

Note that even the smallest airport will normally require some form of communication link to enable submission of biometric data. Even at a smaller airport, consideration should be given to having two badge printers as these are typically maintenance-intensive devices.

If the intention is to have a FIPS 201 compatible enrollment center, then additional requirements apply. (See NIST publications FIPS 201-1 Appendix A regarding PIV processes for identity proofing and registration, and SP800-79-1 Accreditation of PIV Card Issuers.)

It should also be noted that this office typically generates significant paperwork records, which should be appropriately stored and secured.

3) Administrative and Management Locations

In addition to the monitoring and dispatch locations, there is a need to have a location where the access system itself can be administered. This need not be in the control center. At smaller airports, it can be located in the Badging Center. At some airports, it is located with the network control center.

4) Primary and Alternate Operation Centers

Because of the importance of the dispatch center, several airports have chosen to implement two such centers; a primary and an alternate to use in the event that the primary is not available or is disabled. The alternate center need not have the same scale as the primary center, but should have the same system capabilities and connectivity to access control and other systems.

Section III-G—Access Control Checklists:

□ **Emergency Power/Battery Backup**

- All types of servers
- Field control panels
- Operating stations
- Portal hardware
- Credentialing system

□ **Data and Communications**

- Credential system to—
    - o certificated and Federal agents
    - o workstations
- PACS server to—
    - o panel communications
    - o dispatch area
- Field controller to portal
- Physically separate from non-security
- Firewall—PACS to credentialing systems and to outside agents

□ **Security System Infrastructure**

- Separate from non-secure infrastructure
- Controlled access to infrastructure
- Consider encryption on critical links.
- Separate out subsystems by firewalls
- Appropriate access for maintenance
- Secure access for network management

□ **Potential Equipment Placement Locations**

- Terminal area access points
- Secured / AOA / Sterile area doors
- Concourse area entrances (grills)
- In/out baggage doors /controls
- Loading dock doors
- Service corridor and stairwell doors
- Administrative office doors
- Telecom room doors
- Maintenance /equipment room doors

- Tenant and concessions area doors
- Roof / manhole access points
- Fire/emergency exit doors
- Material storage/safe areas
- Display/museum/art cases
- Hazardous material storage areas
- CBP areas (restricted access)
- TSA offices
- EDS operation areas

□ **Duress/Convenience Alarm Locations**

- 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/communication locations
- Parking toll booths

□ **Access Point Locations**

- AOA/SIDA/Secured 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
- Material storage areas
- Parking management/tenant safes
- Critical equipment locations

□ **Money-Handling/Storage Area locations**

- Public Parking and Garage Areas
- Ground Transportation/Taxicab Booth
- Administrative/Reception Areas
- Tenant/Cargo Cash Register Areas
- Airport/Tenant Guard Booths

□ **Credentialing System Checklist**

- Credentialing servers, printers and workstations
- Potential added infrastructure
- Firewall and external connections.
- Physical security of system and supplies
- Selection of appropriate system/agent
- Phasing Plan for eventual interoperability

□ **Biometric access control Checklist**

- Potential for additional infrastructure
- Appropriate biometric and credential technology
- Environmental protection for readers
- Phasing Plan for eventual interoperability

□ **Dispatch Monitoring Location Requirements**

- Secure /separate from admin offices
- Part of integrated dispatch program
- Relevant CCTV access capability
- Alternate monitoring location provided

Section H—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 commitments must be made years earlier. System and equipment specifications drafted during schematic design and development can be superseded by new technology and new standards by the time construction is completed or during the projected life of newly installed equipment.

Planners and designers should systematically monitor technology trends which may impact their systems and determine which near-term developments can be considered for their projects without jeopardizing project performance, schedule, and cost.

References and resources for this section are located in Appendix H, Bibliography.

1. 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 used to monitor a variety of activities and areas, including:

- Area surveillance in terminals
- Roadway and curbside baggage
- Cargo loading docks
- Tenant access points
- Baggage handling areas
- Access to SIDA, AOA, etc.
- Monitor passenger traffic in SIDA
- Gate activities
- Monitoring fenced perimeters
- Vehicle traffic control
- Rental car facilities
- Fuel farm areas
- Parking garage/ lot monitoring
- Employee parking areas

a. Video Standards and Equipment Compatibility

The resolution and frame rates for U.S. and European video standards are shown in *Table III-H-1*.

		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
RS 170	CIF	352	240	8	30
	4CIF	704	480	8	30
	RGB	768	480	8	30
Europe	VGA	720	576	8	25
PAL	QCIF	176	144	8	25
	CIF	352	288	8	25
	4CIF	704	576	8	25
	RGB	768	580	8	25

Table III-H-1—Horizontal/Vertical Resolution of U.S./European Video Standards

For streaming video, the applicable network standard is the widely-accepted Real Time Streaming Protocol (RTSP). For networked video, both wired and wireless transmissions of video are governed by the IEEE 802 series of Ethernet standards which are updated from time to time.

In the analog video world, once a video standard had been adopted (e.g., PAL or NTSC) the user had reason to expect that plugging into matrix switches and DVRs would enable video to be viewed without problems. The video standard, however, did not solve the problems of controlling cameras and lenses, because the control protocols were not standardized.

In the case of IP cameras or analog cameras interfaced to digital encoders, as yet there are no accepted industry standards for interfacing digital video cameras to video analytics or to other elements of an integrated security system, including access control equipment and video storage.

This situation is changing. Two industry groups were formed to standardize protocols for digital video systems: the Open Network Video Interface Forum and the Physical Security Interoperability Alliance. Both groups have published specifications, but their standards are not identical and both require further development.

The standards for digital video encoders are more advanced. For encoding and compressing video streams for network transmission and storage, the currently available industry standards include H.264 (also known as MJPEG-4 AVC), MJPEG-4, and MJPEG.

b. Operational and Technical Issues—Assessment & Surveillance

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.

The performance of a surveillance system depends on a number of factors including:

1) Characteristics of the object to be observed—its dimensions, reflectance, and contrast;

2) Local environmental conditions—atmospheric transmittance (clear, foggy, snow) and turbulence; the level of scene illumination (expressed in foot–candles or lux) and its variation over the 24-hour cycle; the type of artificial illumination (incandescent, metal halide, mercury vapor, sodium vapor, LED, etc.); how the cameras are situated with respect to that lighting, and the presence of strong light sources (street lamps and headlights) and glare in the scene; etc.;

3) Camera characteristics—detector size, sensitivity, signal-to-noise ratio (SNR), modulation transfer function (MTF), spatial resolution (in pixels and TV lines), response to/suppression of bright lights in the scene, etc;

4) Characteristics of the camera objective lens—effective focal length (EFL), modulation transfer function (MTF), wavelengths for which the optics are corrected, and relative aperture (f/#); and

5) Characteristics of the display or monitor—minimal spot size, resolution, contrast, and responsivity.

The “gold standard” for measuring the performance of electro-optical systems is the Modulation Transfer Function (MTF). MTF measures the spatial frequency modulation response of an imager, indicating for each spatial frequency the ratio of the contrast modulation of the output image to the contrast modulation of the input image. MTF is not, however, a practical tool for airport security personnel because of its complexity and because it has no real-world analog, i.e., a person cannot relate MTF values to what he or she actually sees. In addition, commercial video camera and lens manufacturers rarely disclose MTF performance values.

There are two alternative ways to approach design requirements for imaging sensors and specifying their performance:

6) Use “rules of thumb” which the CCTV industry has developed over many years, reflecting industry experience based on actual applications rather than laboratory tests or modeling studies.

7) Use scientifically-based criteria and algorithms, with predicted performance verified by field testing.

Examples of the “rules of thumb” school are 10 vertical TV lines of resolution for reliable detection (“reliable” is not precisely defined); at least three (3) TV lines for motion circuits to detect a moving object in the scene; and at least five (5) TV lines for video analytics performance; and 50 pixels/ft. to see facial features and read license plates under ideal outdoor conditions, increasing to 120 pixels/ft. at night with streetlights.

These rules of thumb can be used to establish baseline values for discussions between users and suppliers, assuming a full video signal and good lighting are available.

An example of the scientific approach are criteria developed by the U.S. Army Night Vision Laboratory, which tested the performance of night vision sensors and developed criteria for real-world imaging performance in the field. While more sophisticated models have since been developed, these criteria survive because they can be applied by non-technical persons.

The criteria describe four levels of imaging performance in terms of the information needed for each level of performance:

8) Detection—the object is present, even of its features cannot be distinguished;

9) Orientation—the longitudinal axis of the target can be sensed;

10) Classification—the class of target can be discerned, i.e., a person can be differentiated from an animal and an estimate can be made as to whether the object is male or female; and

11) Identification—target characteristics within a class can be determined, e.g., a person can be recognized.

Table III-H-2 highlights the increasing amount information (resolution) required to move from detection to identification. The table includes two levels of confidence (probabilities) for each level of performance.

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

Table III-H-2—Resolution per Minimum Target Dimension in Line-Pairs

(1 line pair = 2 pixels; 2 pixels = 1 TV line)

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.

c. Selecting Equipment—CCTV Cameras

Previously, detectors in most surveillance cameras used tube technology. 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 technology developed for personal computers. CMOS technology dominates megapixels camera detectors for these reasons.

Camera performance is a function of scene illumination, how a camera is positioned and mounted to view the scene, and target properties. Scene illumination is especially critical at night. Visual-band cameras sense reflective light; the amount of reflected light depends on natural illumination, often augmented at by artificial lighting, and the contrast and reflectivity of targets. 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.

For very low-light conditions, CCDs and CMOS arrays can be fitted with image intensifier modules to operate down to starlight scene illumination levels. Intensifiers can significantly increase acquisition costs and also reduce operational life of the camera. Adding supplemental visible lighting to permit the use of normal CCD/CMOS cameras should be considered as a cost-effective alternative to using intensified cameras. Another alternative is the use of thermal imaging (infrared) cameras.

The common sizes of CCD/CMOS camera detectors eras are shown in *Figure III-H-3.* Detector size, and the horizontal dimension of the detector in particular, plus the focal length of the camera's objective lens, determine the surveillance field coverage of a camera and the distance at which an object can be imaged. Array cost is primarily a function of the number of good arrays a manufacturer can realize from a silicon wafer, i.e., the yield factor. Cost is generally proportionate to yield (number of good chips per silicon wafer), and this favors the smaller array sizes. As a result, most surveillance cameras use 1/4-in and 1/3-in arrays, especially dome cameras where compact size is important.

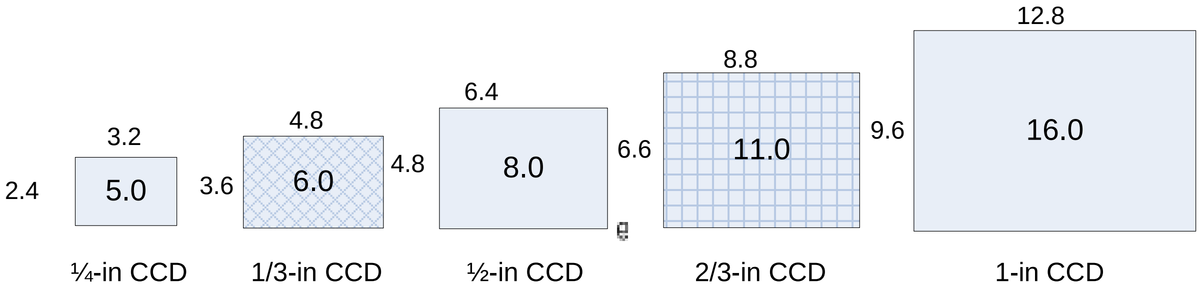


Figure III-H-1—Dimensions of CCTV Detector Arrays

Dimensions are in millimeters (mm)

Camera detector size and lens focal length selection should be determined by what is to be viewed, at what distance, and with what resolution. In some instances the angular or horizontal coverage of the camera will drive the design, especially for outdoor area coverage. In other cases, the ability to resolve target details will set the requirement. Selection can also be limited by physical space availability, e.g., dome camera dimensions are more restrictive than box camera housings.

For cameras equipped with zoom objective lenses, magnification is often given as a combination of both optical zoom and electronic zoom. Increasing the focal length of a zoom lens will result in more "information" from the target being focused on the detector. Increasing the apparent magnification electronically, however, simply increases the size of the pixels and adds no new "information" about the target, so it is not a substitute for optical zooming.

Video surveillance cameras should be sited for overlapping coverage to the extent practicable, as protection against any camera failing and also to provide alternate views of objects to enhance their detection and tracking. The extent of overlapping coverage can readily be determined from a Web-based camera-lens calculator and shown diagrammatically. *Table III-H-4* shows how horizontal angular and linear field coverage varies with detector size for a sampling of objective lens focal lengths. Coverage is a function of detector width and lens focal length.

	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	5.0	6.7	9.8
100	1.8	2.7	3.7	5.0	7.3
200	0.9	1.4	1.8	2.5	3.7
300	0.6	0.9	1.2	1.7	2.4
500	0.4	0.6	0.7	1.0	1.5
1000	0.2	0.3	0.4	0.5	0.7
Lens Focal Length (mm)	Linear Field average at 1000 feet				
5	640.0	960.0	1280.0	1760.0	2560.0
10	320.0	480.0	640.0	880.0	1280.0
25	128.0	192.0	256.0	352.0	512.0
50	64.0	96.0	128.0	176.0	256.0
75	42.7	64.0	85.3	117.3	170.7
100	32.0	48.0	64.0	88.0	128.0
200	16.0	24.0	32.0	44.0	64.0
300	10.7	16.0	21.3	29.3	42.7
500	6.4	9.6	12.8	17.6	25.6
1000	3.2	4.8	6.4	8.8	12.8

Table III-H-3—Horizontal Angular & Linear Field Coverage of Surveillance Cameras

For airport operations, the parameters of a CCD/CMOS camera which are operationally significant include:

12) 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.

13) Effective picture elements (pixels): The number of horizontal pixels times the number of vertical pixels in a scene.

14) Minimum resolution: The smallest division, to which a measurement can be determined, generally expressed as TV lines.

15) 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.

16) 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 are likely to occur, airport security in the ConOps requirements should advise the surveillance system designer of such conditions.

17) Some color cameras now change automatically to monochrome operation, in order to maximize resolution, when a low-light illumination threshold is reached.

18) Dynamic range: The ratio of the full-scale range of a data converter to the smallest difference the detector can resolve. Dynamic range is generally expressed in decibels. Operationally, for airport security it will be important to have sufficient dynamic range to operate from minimum illumination, such as street lamps at night, to full sun conditions. In high sun environments, this may require the use of neutral density filters in the lens to avoid saturating the camera detector if the maximum illumination cannot be controlled by a mechanical iris.

19) Signal-to-noise ratio: The ratio of total signal to electronic noise expressed in decibels (dB).

20) Minimum scene illumination: For a given lens f/#, the minimum amount of scene illumination required to produce an image at full video bandwidth.

21) Backlight compensation: The dynamic range available to prevent a backlit subject from darkening an image or saturating the detector. This parameter is important when strong point light sources are present in the scene.

In most cases, a camera can be used inside a facility as well as outdoors, the difference in configuration being the type of housing required for the particular environment. Lighting is also a factor. Light levels indoors generally vary over a small range, whereas outdoor conditions may vary widely over the day-night cycle depending on the extent of auxiliary lighting used. Where camera design requirements converge, consider using the same cameras indoors and outdoors to simplify training and maintenance and to minimize replacement costs.

Indoor environmental conditions are generally under the airport operator's control. In most instances, special environmental conditioning should not be necessary. Housings still may be required to protect cameras from accidental or deliberate damage, even to the extent of armoring cameras against weapon attacks, and all such housings should include locks.

Exterior (outdoor) cameras will be subject to local temperature, wind, rain and snow. They may also be installed on poles or sides of buildings where access is difficult. Cameras 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.

2. IP (Internet Protocol) Cameras

IP cameras are network-ready imaging appliances. Depending on the operational requirements of the surveillance system, IP cameras can simplify the network infrastructure by enabling video, control signals for PTZ units, and even electrical power to be transmitted over the Ethernet cable plant, thereby saving the expense of installing separate power and control cabling.

In an IP camera, the video signal is digitized internally and compressed for transmission over the network. Storage may also be embedded in the camera to reduce transmission bandwidth use.

The IEEE Power-over-Ethernet standard defines the means of powering IP devices over Ethernet cabling. The 802.3at standard enables 30 to 60 watts of power to be delivered to devices in this manner. This assumes that the IT network is already installed or expensed; that it has sufficient bandwidth for the number of cameras to be put on the network; that it has adequate performance quality (latency, jitter, and dropped packets) and security; and that network nodes exist at or in proximity to the IP camera. If a separate IT network is to be installed for the security system, that cost should be factored into the system design trade-offs done during schematic design.

Monitor capabilities cannot be overlooked in system design. IP cameras may provide better image quality, compared to using analog cameras with separate encoders, but such differences will only be apparent if the user's monitor can display the difference in camera resolution. In addition, many cameras record at 2CIF resolution, and most video analytics are based on 2CIF resolution, further reducing any differences among cameras. Comparing only camera specifications may be misleading—the evaluation should be done in a system context, not a camera context.

Many dome cameras and other types which use 1/4-in and 1/3-in CCD arrays are available as IP cameras. Few 1/2-in format IP cameras are and this situation is not expected to change. Megapixel cameras are generally IP cameras and mostly use CMOS detectors because of yield and cost issues.

Installing and/or transitioning to IP cameras can be challenging. There are as yet no agreed-upon standards, and implementations differ among manufacturers with regard to video streaming, configuration, status notification, and other features. An installation plan, supported by a system acceptance test plan, is essential to realizing the desired system performance objectives.

3. Megapixel CCTV Cameras

"Megapixel" refers to cameras having arrays with a minimum of 1 million pixels, and at the present time includes cameras with up to 16 million pixels.

The arguments for megapixel cameras are:

a. Very high resolution: The increased pixel count gives much better quality image for both forensic and legal purposes; there is little benefit to capturing a criminal in the act if the resolution does not enable the criminal to be identified.

b. PTZ Alternative: A single fixed megapixel camera equipped with a wide angle lens, or with a motorized zoom lens, may be able to monitor large outdoor areas, such as parking lots, or long indoor terminal concourses, which otherwise would require multiple fixed cameras. A megapixel camera can do this because the video image can be zoomed electronically, by three times or more depending on the pixel count, and still yield acceptable image quality on the user's monitor.

c. With some megapixel cameras, electronic zooming also enables an image-within-an image to be created in real time. A user can designate an area of interest in the field of view and magnify an object within that area while still viewing the entire field coverage in the background, thereby retaining situational awareness across the area under surveillance. Zooming in on an object with a PTZ camera, by contrast, narrows the field coverage and carries a corresponding loss of situational awareness.

d. Reduced Costs: Using a few megapixel cameras instead of a larger number of conventional cameras can reduce system acquisition and support costs.

Operationally, a potential user should be aware of the following issues when considering the use of megapixel cameras.

1) The current offerings of megapixel cameras vary widely from manufacturer to manufacturer with respect to array size (number of pixels), software enhancements (such as image-within-an image), and compatibility with third-party equipment such as elements of video management systems (VMS) and analytics software—factors which complicate the selection and integration process.

2) While often cost-effective for area surveillance, especially when maintaining situational awareness is important or when forensic-quality imagery is required, megapixel cameras are generally not cost-effective for basic tasks such as monitoring doorways.

3) A larger number of pixels does not guarantee mega-imagery detail. Some operational conditions will result in much less detail than would be expected by the pixel specifications, particularly when a camera is operating under less than ideal conditions such as poor lighting.

4) Current models of megapixel cameras generally do not perform well under low-light conditions, or in the presence of very bright lights. Expectations of a reduction in camera count may not be realized if night illumination is inadequate, thereby reducing field coverage and/or target distance. Where night surveillance is required, megapixel camera performance can be enhanced by upgrading a lighting system, which may be less expensive than using alternative imagers such as intensified CCTV cameras or thermal (infrared) imagers.

5) Megapixel cameras require higher quality, more expensive objective lenses than conventional cameras because of their small pixel dimensions. For large format megapixel cameras, including 1-inch arrays, the range of megapixel-qualified lenses is currently limited, and installing a lens designed for a smaller format will crop the image.

6) The range of third-party video analytics for megapixel cameras, independent of the camera manufacturer, is limited at the present time.

7) Even with H.264 video compression, which is only recently becoming available for megapixel cameras, storage requirements will be much greater than for conventional cameras.

8) In the absence of agreed industry standards, megapixel cameras pose the risk for a user to be locked into a proprietary, single-source solution.

Megapixel cameras offer advantages for specific situations, and should be considered in that context rather than as a universal solution to every application. The additional marginal cost of megapixel cameras in those locations which require them, may be small compared with the total cost of ownership of the CCTV system over its expected life.

4. CCTV Camera Lenses

Camera lens types can be classified as:

a. Fixed focal length lenses. The lens is manufactured to a specified focal length selected for the particular application.

b. Varifocal lenses: The focal length of a lens can be adjusted manually over a specific range, e.g., between 25 and 100 mm, to tailor its coverage to the scene to be monitored.

c. 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 lens parameters to consider include:

- Effective focal length (EFL), expressed in millimeters (mm)—EFL determines the angular field of view (degrees) and linear field coverage (feet or meters) and viewing magnification.
- Relative aperture, commonly known as the f/#—the ratio of the lens EFL to the diameter of its clear aperture, and the measure of lens light gathering capability. The f/# 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 f/# is normally stated at the minimum EFL setting, e.g., f/1.4 at 25 mm. As EFL increases so will the numerical f/#. Zooming a lens from 25 mm to 100 mm, for example, will increase the numerical aperture from f/1.4 to f/5.6, reducing the amount of light gathered significantly to the point where a camera may not function under poor lighting.
- Optical correction—not all lenses are equal, and lens quality should be carefully considered when using megapixel cameras which have smaller pixel dimensions than conventional camera arrays.

5. Thermal Imaging (Infrared) Sensors

Thermal, or infrared, imagers sense target radiation as compared to visible wavelength CCTV cameras which sense reflected light. There are four transmissive “windows,” or bands, in the electromagnetic spectrum which can be used for imaging:

a. Near-infrared (NIR)—0.75-1.4 µm (microns), commonly used in fiber optic telecommunication because of low attenuation losses in the glass (silica) medium. For imaging, image intensifiers and intensified CCTV arrays use this band.

b. Short-wavelength infrared (SWIR)—1.4-3 µm, beyond which water absorption increases significantly. The 1,530 to 1,560 nm range is the dominant spectral region for optical fiber used in long-distance telecommunications, but it is not an atmospheric imaging band.

c. Mid-wavelength infrared (MWIR)—3-8 µm, historically one of the two most popular bands for infrared imagers and the band of choice when target resolution is a priority.

d. Long-wavelength infrared (LWIR)—8–15 µm, the other popular band for infrared imagers and the band of choice for imaging during poor weather conditions or in the presence of some types of smoke.

Thermal imagers are most often used for outdoor surveillance under conditions where the level of visible light illumination and/or poor weather will significantly degrade the performance of visible CCTV cameras.

Until recently, thermal imagers were only available in the MWIR and LWIR bands and in two types: imagers with uncooled detectors and imagers with detectors having cryogenic coolers. Thermal imager selection involves a trade-off between performance and price; cooled detectors offer better performance but are more costly because of their cryogenic coolers, whereas the less costly uncooled detectors may require larger, and more expensive, optics.

The optics of these imagers use crystals, such as germanium, which transmit infrared energy. Conventional glass optics block infrared energy so thermal imagers cannot see through glass windows. Infrared optics are more expensive than glass lenses for this reason.

The performance-price trade-off favors uncooled imagers for targets at distances of one 1 km or less, and cooled imagers for targets at distances greater than 2 km. For targets between 1 and 2 km, the selection will be governed by the bidding process plus operational factors such as reliability and maintainability.

SWIR imagers are relatively new but offer near-CCTV resolution with the ability to image under low-light conditions, plus some capability to penetrate smoke and light fog (although not as much as provided by longer wavelength MWIR and LWIR imagers). Depending on the optics used, SWIR imagers can see through glass windows—which are not possible with MWIR and LWIR imagers. The availability of SWIR detectors and lenses designed for t hem are currently limited but are expected to increase in the coming years. For security applications where poor weather is infrequent and where target resolution is the main objective, the SWIR band merits consideration during schematic design.

Operationally, it is important to understand the relationship between infrared wavelength and imager resolution. Imager resolution is proportional to the inverse of wavelength. For imagers having the same lens focal length, on a monitor the resolution (detail) of an MWIR image will typically appear to be about one-third that of a CCTV camera or NIR image intensified array and an LWIR imager will appear to have about one-tenth of the resolving power of a CCTV image.

Operationally, it is also important to consider how imager performance is affected by environmental factors. Thermal imagers sense temperature differential; if a body is at the same temperature as the environment, it may not be “seen” by the imager or the detection distance may be greatly reduced—a situation to be addressed in specifying thermal imagers for warm climate operations. For operations in rainy and snowy conditions, the clothing of persons in the scene may absorb sufficient amounts of moisture to effectively mask their body temperatures, reducing detection ranges. For operations in fog, the density of fog will affect detection performance and this will vary with the band of operation. Similarly, in the presence of smoke, the chemical composition of the smoke as well as its density will affect detection performance.

6. Intelligent Video

Intelligent video refers to imaging enhancements which exploit a camera's output signal. Intelligent video originated with motion detection. Circuits in the camera or in an external appliance monitor changes in the level of the video signal in a designated "area of interest" drawn electronically on the monitor. An operator can then be alerted to an event as it happens, greatly reducing the need for operators to stare at video monitors for long periods of time.

The effectiveness of this technology has improved greatly. Systems now are able to compensate for the sun progressing across its arc during the day and for environmental effects such as blowing trees, which created false positive alerts in early systems. Intelligent systems can also detect multiple objects in a scene, and exclude designated areas of a scene; track objects as they move across the scene; generate position coordinates and speed data for these objects as they move; and in some cases distinguish types of targets by class, e.g., distinguishing between humans, animals, and vehicles. How valuable these functions are depends on the user's operational requirements (preferably determined in the ConOps) and, especially, how reliably they perform, i.e., the false alarm rate.

Intelligent video functions apply mainly to fixed cameras, but under certain conditions, object detection and tracking can span multiple cameras even as these cameras are panned and tilted.

Intelligent video is also able to analyze an object and make a determination if it is possible threat, based on behavioral "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, a camera monitoring that jetway will see the change in course and use object tracking software to notify an operator in the Security Operations Center. 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.

The key to "fusing" these sensor inputs is showing them on monitors, or a video wall associated with one or more live images and layout diagrams, including maps and engineering drawings which can be animated. An even more advanced "fusion" process shows the airport in graphic form starting from a point above the airport and zooming, electronically, down to a specific access point based on alerts from access control devices or radio frequency tags (RFID). Using this technology, persons or devices, including baggage, which have RFID tags can be tracked across an airport using wireless networks and be located precisely at all times.

All of these features and advanced capabilities come at a price. During development of the ConOps, airports need to carefully weigh the benefits and costs, especially with regard to how these features contribute to established operational requirements, how they are to be implemented, and their downstream support requirements.

Intelligent video capabilities which are implemented entirely in software may have a cost advantage, depending on software licensing rates, but may also impact hardware by requiring more powerful servers and increased hard drive capacity, or a reduction in the number of video cameras which a server can support simultaneously.

A program implemented as a new hardware appliance may impact available equipment space, electrical power, and network interfacing, in addition to requiring 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 two attempted intrusions of multiple 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 monitors in the SOC; and
- Demonstrate 3D visualization of the events, in real time, on the operator monitors.

7. Video Analytics

Video analytics are a form of intelligent video in which decision rules, implemented in software, apply specific behaviors and/or changes derived from the video signal.

When properly configured, video analytics can greatly enhance video surveillance capabilities and reduce the workload of monitoring personnel, but they should be carefully planned and installed, with appropriate training. Video analytics performance is sensitive to viewing conditions including lighting, weather, camera angle, distance to a target, activity in the camera field of view, and changes in the viewing background. Users should assume that proposed video analytics have been designed to function with full video signals (100 IREs and 50dB SNR or greater) unless the manufacturer is able to provide data on performance under less than optimal lighting and environmental conditions.

False alarm rate is the driver for user acceptance of video analytics. Even in a relatively small network of 100 cameras, one false alarm per camera per day will often cause a user to turn off the analytics. It is the A&Es responsibility to document how the analytics are to perform, how they are to be tested to verify how the analytics will perform across the user's conditions, and how they will benefit the user. In some cases, operational performance can only be determined by testing across the range of local operational conditions found at the airport.

There is no substitute for testing candidate cameras and candidate analytics in the user's environment, preferably over a period of at least several days and different conditions, during or prior to schematic design. The testing should validate camera compatibility and the extent to which the analytics can be "tuned" to achieve an acceptable, to the user, false alarm rate.

Even the type of artificial lighting can affect analytics performance. For example, sodium vapor lamps commonly used for street lighting have a very narrow spectral distribution centered at 590 nm. There is very little area under the spectrum curve, which limits the energy which a camera can detect. Changing from sodium vapor lamps to modern light emitting diode (LED) lamps, which have a broad color distribution, can be the difference between useable and unusable video analytics under nighttime conditions. The analytics should be able to "learn" and apply environmental variables and suppress false alerts without sacrificing performance. Reducing sensitivity to minimize false alarms is not a viable solution if it also reduces performance below what is needed.

Video analytics can be associated with both color and monochrome video cameras as well as with thermal (infrared) cameras. Typical applications are:

a. Associated with Fixed Cameras
   1) People congestion.
   2) People counting.
   3) Abandoned object detection.
   4) Human tailgating.
   5) Basic detection, i.e., monitoring a portal.
   6) Parked vehicle detection.
   7) Advanced motion detection for determining the direction of vehicle and human intruders.

b. Associated with PTZ Cameras
   1) PTZ scan and dwell modeled for vehicle and human intrusion.
   2) Fixed to PTZ handoff for target tracking, e.g., handing off an image from a fixed camera to follow a moving target.

Each of the analytics functions selected by a user should be specified, including how the function will be assessed and validated during acceptance testing.

There are two general ways in which video analytics may be configured:

- Server-based analytics, in which the software runs on servers in the data center or SOC, and

- Camera-based analytics, in which the software is embedded in cameras at the edge of the IT network, in some instances with video storage also being embedded in the cameras.

There are pros and cons to both approaches, with potentially significant operational and maintenance cost implications. During schematic design, both approaches should be evaluated against the user's operational requirements and the architecture and capabilities of the IT network which is to support the video cameras.

Server-based analytics leverage the computing power of modern IT servers, storage devices, and maintenance availability in the IT datacenter. Server-based analytics enable a user to select best-of-class analytical software independent of camera capabilities; it is unlikely that any one manufacturer will have best-in-class software as well as the cameras best suited for specific applications. At the same time, a server may support several cameras so loss of the server will mean the loss of multiple cameras. This also applies to centralized video storage devices. There are ways to buffer such problems but they introduce their own complexities and costs.

Server-based analytics buffer the user from a closed, proprietary, single-source video solution which may have limited upgrade potential, and which would be expensive to replace if problems develop with either the analytics or the cameras (or the manufacturer goes out of business).

Camera-based analytics leverage compression at the source, reducing the bandwidth required for video transmission over an IT network. Storage may also be embedded in the camera. By also incorporating solid-state storage chips for short term storage with hard drives for longer term storage, the hard drives will run only for short periods of time, extending their life and improving their reliability (a major issue with video hard drives, which typically run 90 percent or more of the time in "write" mode). For outdoor cameras, all embedded elements must meet local environmental requirements and, in a desert or tropical area, this may require supplemental cooling. Being able to service remotely located cameras, some of which may to be mounted atop poles, is an issue when the camera contains the "smart" components of a video network.

The advantages claimed for embedded analytics, with or without embedded storage, can also be realized by performing the analytic functions in an appliance installed at or near a camera, with or without local storage. Such an appliance could support one or more cameras depending on where the cameras are installed and their accessibility to a network node. Use of an external appliance for compression, analytics, storage, and network security (firewall) will enable any type of camera and any compatible analytics software to be selected, thereby eliminating the user's dependence on a single-source supplier.

Having access to multiple suppliers can be a considerable benefit for an airport and especially when complex, evolving technology is involved.

8. Video Encoding and Compression

How a video stream is compressed and stored in digital format depends on (a) the type of video camera, (b) the storage architecture, and (c) if the video is transmitted over an IT network, the available network transmission bandwidth.

More than 90 percent of the CCTV cameras installed worldwide are analog cameras. The percentage is even higher for thermal (infrared) cameras. In the case of CCTV cameras, the percentage will decrease as more IP cameras are installed, but in the near term, analog cameras will dominate the installed base. Encoders will still be needed to digitize and compress streaming video for transmission over digital networks and to integrate with video storage devices. Encoders will also provide the interface between analog cameras and DVRs, and to interface with video management systems (VMS) which do not support DVRs.

Realizing the benefits of video compression protocols and avoiding problems or image degradation requires consideration of scene complexity, streaming mode, video frame rate, and how the compression protocol is configured and applied (constant and variable bit rates and levels of quantization), and other parameters.

There are several video compression protocols available. The most commonly used are MPEG, MJPEG-4, and H.264 (also known as MJPEG-4 AVC) compression protocols.

MJPEG-4 is currently the mostly widely used video compression protocol, offering proven performance with stable operation.

The H.264 protocol is rapidly becoming the compression standard of choice for surveillance video because, under most conditions, it provides better compression with comparable image quality compared to MPEG-4 when images are viewed on a monitor. The compression advantage of H.264 may be important if network transmission bandwidth is an issue. H.264 can also reduce hard drive storage requirements, although even terabyte capacity hard drives are now relatively inexpensive.

The H.264 protocol is available in several types, and the ratio of full frames to incremental frames can be varied, affecting CPU requirements as well as viewing quality. H.264 quality is sensitive to frame rate; at 7.5 fps, the small number of full frames may affect viewing quality as well as the functioning of video analytics under less than ideal conditions. For scenes with high levels of activity, similar problems may arise at 7.5 fps. For these reasons, setup should be carefully addressed and, if any doubts arise, the proposed configuration be subjected to testing with the intended cameras and encoders to assure that the specified output quality will be realized.

If IP cameras are used, the digital conversion and compression will normally be done at the cameras, with the output formatted for transmission over a local area network. In this case, the bandwidth and processing capabilities of the camera electronics will determine the maximum resolution and frame rate 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.

9. Video Management Systems (VMS)

In enterprise-type security systems, video cameras almost always distribute video to viewing stations and storage media through a video management system (VMS). A VMS manages video images received from multiple cameras across a network. It then enables the user to operate on the video streams, distribute the video, store the video, and perform other functions.

A VMS may store video in several ways. Digital Video Recorders (DVRs), which serve analog cameras, or on Network Video Recorders (NVRs), which serve IP cameras (hybrid DVRs have recently been introduced which support both IP and analog cameras), are commonly used, but it is also possible to directly write to network storage systems (see the discussion of NAS and SAM under Storage).

A VMS which includes DVRs and NVRs may lock the user into a proprietary solution, i.e., limiting the choice of cameras, video analytics, and other video elements to those available from the DVR or NVR manufacturer.

A software-base VMS solution is an application package designed to support many video hardware packages and is designed to support many camera, DVR, and NVR manufacturers. These applications typically provide a long list of functions, which is both good and bad—good because it gives an operator a wide range of capabilities, and bad because the demands on the operator, and the associated training required, increase with complexity.

A rule-of-thumb for VMS systems is that 80 percent of the operators use 20 percent or less of the advertised features. Having a long list of available functions does not mean that all of them will be used or that all of them are needed. The key, during schematic design, is to identify what functions are really required and then select a VMS which provides them in the most user friendly manner, with the least complexity, and preferably using open standards.

There are no industry standards for VMS systems or how they are configured. VMS architectures differ widely, as does support for third-party cameras and video analytics. Indeed, some VMS “packages” only support the manufacturer’s own cameras and analytics, which would prevent a user from specifying third-party products and poses sole-source procurement and support risks. If a user intends to specify cameras and video analytics independently of the VMS, the VMS provider, which for enterprise systems may be a system integrator, should be required to guarantee interoperability of all video elements (hardware and software) and back this up with a demonstration which also includes setup procedures, matching features to user requirements, and ease of use.

Some of the other issues to be considered and evaluated when assessing VMS suitability and how well a particular VMS meets the user’s requirements for a video surveillance system include:

a. Architecture. Most VMS systems use a client-server architecture. If the central servers fail, so does the entire system unless the manufacturer includes failover measures and redundancy. The alternative is to use a peer-to-peer architecture, but this requires that the distributed databases be properly synchronized. What measures are provided and how they are applied should be evaluated.

b. Basic Functions. A VMS provider should demonstrate how cameras are called up, how images are monitored and processed, how images are stored and recalled, and how third party applications are integrated into the operator screens. In some VMS, many functions can be accessed with a few clicks of a mouse, while in others the operator may have to click through several layers of menus on the screen. Menu-driven applications may afford greater flexibility but where extensive menu trees are involved, more capable operators and more intensive operator training may be necessary. Accessing third party applications, such as video analytics, may differ from the VMS methodology and may require entirely different setup procedures. The user should become familiar with all of these functions and the operator menus to access them during the assessment process.

c. Feature Set Customization. The software should enable a user to lock-out all but the most needed features and do to this for each operator station.

d. Scene Viewing. Some VMS systems offer scene stitching, which allows an operator to stitch or merge the imagery from multiple adjacent cameras and can greatly assist it coping with areas of high activity. The user should decide if this feature is important.

e. PACS and IDS Integration. All VMS systems offer some level of integration for alarms and events, but the extent of integration and how the data are presented, e.g., with or without geo-referencing overlaid on photos and/or CADD drawings of the facility should be demonstrated to the user's satisfaction.

f. VMS Throughout. For large systems, how the VMS manages heavy loads and stresses on the system should be evaluated. The VMS should enable a user to apply rules for prioritizing different types and locations of traffic under these conditions.

g. Investigations and Case Management. Most VMS systems provide only basic search and investigative functionality. The user should decide if search and case management capabilities are important.

h. Monitoring and Auditing. All VMS systems log activity data and provide for recall and analysis of the event data, but the implementations vary widely. User requirements for these functions also differ, which complicates the necessary evaluation process.

VMS pricing also varies widely, ranging from single-server licenses to multi-tiered license structures for different levels of functionality. There is no "price per function" metric available to assist a user in making a value assessment, i.e., comparing functional capabilities to their associated prices.

10. Video Storage

Video storage, whether in analog (tape) or digital (hard drive, optical media, or tape) formats, can present significant design, management, and cost challenges, especially for airports having several hundred or more video cameras.

The first step, during the ConOps, is to determine what video must be stored, for what period of time, and at what quality level. These are operational, not technical, requirements and they include assessing the frequency and consequences of potential threats. At this time, there are no approved standards or TSA regulations that govern how an airport operator is to define and apply them.

In a digital network environment, video streams will be compressed either at the edge of the network or on centralized servers.

Video may also be stored at the edge, in cameras or in edge appliances, to reduce network bandwidth requirements, but this is temporary storage and not "record" or archival storage.

The network video streams may include all frames as well as frames "tagged" as motion frames or video analytic frames. The user can choose to store all video frames in several ways depending on the requirements defined in the ConOps. For example, all video, including motion video, could be stored for one or more days so that if an event occurs, what took place before and after the event will be available for examination; or store all video frames for one or a few days and only "tagged" frames for a longer period of time. There are many possible scenarios that might be considered.

Many airport operators have elected to store video for 30 days, but this is not a standard. Other airports store video only for seven days while, in extreme cases, a year or more may be driven by policy concerns including public safety and risk management.

Typically, motion or video analytics frames represent 15 to 20 percent of all frames—the other frames representing "no action" and routine surveillance.

Storing only “tagged” frames for all cameras after a few days can significantly reduce video storage costs, equipment rack space, electrical power including UPS backup and HVAC cooling, and system management. Unless there is a compelling reason to store all frames for more than a few days, storing only tagged frames after a time determined during the ConOps will better serve the airport’s interests.

Digital video streams can be transmitted at full video frame-rate, which in the United States is 60 frames/ second (fps), and also at a reduced frame rate which can be as low as 1 fps. If video analytics are used, the frame rate should be at least 7.5 fps with 15 fps used for areas of high activity. The video analytics vendor should confirm this and demonstrate that it works properly.

Depending on the VMS capabilities, it may be possible to also capture “tagged” frames at a reduced frame rate after several days, further reducing storage equipment acquisition and support costs. These are measures to be examined during schematic design.

Internal storage, using DVRs and NVRs, lack the capacity to support store the outputs of hundreds of cameras over a typical 30 day scenario. Attached storage, using external hard drives, is likely to be needed for large video surveillance systems. The two most common types are NAS (Network Attached Storage) and SAN (Storage Area Network) that are arranged in modular clusters that are scaled for the required amount of storage, that employ RAID (Redundant Array of Independent Disks) for protection against hard drive or power failure, and that are networked over the LAN.

The configuration, capacity, networking and equipment required for video storage are properly determined during schematic design. For large video systems, storage clusters should be less expensive than cascading DVR and NVR units, be easier to manage, provide higher levels of reliability using hot-swappable components and reconfigurable-on-the-fly volumes, and be more compatible with the use of megapixel cameras.

Streaming video is a write-intensive storage process, and standard hard drives were never designed for this type of operation. Some hard drive manufacturers offer so-called AV-class (for audio-video) hard drives for video storage which claim higher reliability and provide longer operating warranty periods at nominal increases in cost. The selection of hard drives should consider such products during schematic design.

The system may also include off-site storage for protection against catastrophic events at the airport, such as floods or a terrorist attack, the need for which should be determined during the ConOps.

For airport video to serve the needs of law enforcement, the means of storage and access to the stored imagery will require special attention once image quality requirements have been resolved. If the video imagery is stored digitally, issues of “secure storage” and information “authentication” will arise and will require that the airport establish consistent, valid, and verifiable procedures for controlling access to, and authenticating, the digitally-stored imagery. A digitally-stored image 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. If file encryption is to be used, a U.S. Government approved technique such as the Advanced Encryption Standard (AES) should be considered.

11. System Design and Infrastructure

Typically, video surveillance systems have been designed as components of a broader facility security system or sometimes as stand-alone systems. 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 be transmitted over the network infrastructure, assuming adequate transmission bandwidth exists for the number of cameras involved.

System planning should also address the following system and operational issues:

a. Privacy Protection. Security system design should provide for the control of internal permissions and authorizations for access to data, and permissions over activities like the copying and disseminating data. There also need to be supervisory and audit controls designed to mitigate the possibility of misuse of data

b. Records Retention. Planners and designers should address retention requirements established by the ConOps, including possible Freedom of Information Act requirements and forensic requirements.

c. SSI Regulation. Schematic design should address the extent to which video imagery is covered under TSA SSI regulations and ensure that SSI data are properly identified and safeguarded, including permissions and authorizations with respect to access, use and dissemination of video data.

d. Video Quality. Airport security normally does not require "identification" quality video imagery, in contrast to law enforcement which focuses on identifying persons. As the standard criteria indicate, "identification" quality video requires several times more "information" than detection, orientation, or recognition video, which translates into more capable, and more costly, video surveillance cameras, lenses, and storage devices. During development of the ConOps, specific locations where "identification" quality video imagery will be required should be identified and tagged for schematic design. It may also be necessary to establish a chain of custody of video data that is going to be utilized as evidence to ensure the integrity of that data.

12. Lighting & Special Operational Conditions

Whether lighting is exterior or interior, the placement and amount of lighting should 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.-candle 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 now commercialized, is the use of light emitting diodes (LEDs). LED lamps are now widely used for highway lighting and for illuminating critical infrastructure assets on government facilities. These solid-state devices are smaller and use much less power than conventional lamps for equivalent outputs. Their broad spectra also match the sensitivity of CCD cameras better than the spectra of sodium vapor lamps.

The lighting industry has set a goal for white LEDs output of 150 lumens per watt (lm/W) by the year 2012.

For airports, replacing sodium vapor lamps along perimeters can enable high-sensitivity CCD cameras to function with video analytics at night, thereby avoiding the cost of installing power-intensive infrared illuminators, expensive intensified cameras, or thermal (infrared) imaging cameras.

LED lamp fixtures are available in units which can replace sodium vapor lamp fixtures in the field without having to upgrade the local electrical infrastructure.

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 and, if implemented, video analytics, to function properly under these conditions should then be tested in an operational environment.

<u>Section III-H—Surveillance and Video Detection Systems Checklist</u>:

□ **Set Operational Requirements per ConOps**

Review surveillance site requirements

Determine resolution and field for

- ▸ Detection
- ▸ Orientation

Classification

Identification Camera placement and mounting

- ▸ Fixed or movable (tracking)
- ▸ Security
- ▸ Access—maintenance

□ **System Design and Equipment Selection**

- ▪ Balance
    - ▸ Operational/functional requirements,
    - ▸ cost,
    - ▸ security
- ▪ Camera types and applications
    - ▸ Imaging technology

Analog-IP-CCD-CMOS-thermal

Configuration-std/megapixel

- ▸ Powering and networking standard or IP-based

- ▪ Intelligent Video Functions enhance performance, reduce labor
    - ▸ Target Tracking
    - ▸ Video Analytics
    - ▸ Video Management Systems
    - ▸ Configuration—server-based vs. embedded
- ▪ Lighting
    - ▸ Exterior Perimeter
    - ▸ Interior Areas
    - ▸ Infrared (non-visible) Lighting
- ▪ Video Storage
    - ▸ Hard drive selection
    - ▸ Resolution
    - ▸ System configuration
- ▪ NVR vs. DVR, NAS or SAN
- ▪ Hardware/software compatibility/interoperability
    - ▸ Compatibility w/industry standards
    - ▸ Interoperability of all elements

□ **Other System Issues**

- ▪ Retention, access, and protection
- ▪ Information Retrieval and Distribution
    - ▸ Privacy
    - ▸ Statutory Constraints
- ▪ Reduce LEO response requirements
- ▪ Power/Data
    - ▸ Power—emergency operations
    - ▸ Battery backup not required
- ▪ Camera Installations—derived from operational analysis of surveillance required
    - ▸ Ticket Counters & kiosks
    - ▸ Terminal Apron
    - ▸ Security Checkpoint
    - ▸ Public Lobby
    - ▸ Curbside Baggage
    - ▸ Loading Dock/Police Parking
    - ▸ Administrative and Tenant Areas
    - ▸ Airside Access Doors and Gates
    - ▸ Baggage Handling and Claim Areas
    - ▸ FIS Areas
    - ▸ PACS Access Points
    - ▸ Runways/Taxiways
    - ▸ Cargo/GA/FBO Ramps
    - ▸ Public and Employee Parking

□ **Procedures and Personnel**

- ▪ User-Friendly Design
- ▪ Maximum 4 Monitors per Operator
- ▪ Training Plan
- ▪ Emergency Ops & Maint. Plan
- ▪ Planned Maintenance/Outage Plan
- ▪ Equipment Service Tracking
- ▪ Periodic Upgrade/Evaluation

Section I—IT, Power, Communications, Cabling Infrastructure & Cyber Security

1. Introduction

Prior to this section we have been dealing with design guidelines specific to functional areas of airport security systems. This section focuses on several critical supporting infrastructure elements such as Power, Communications, IT and Cabling Infrastructure, as well as cyber-security and other logical functions. These elements are essential to support an airport enterprise architecture that hosts multiple, and potentially integrated, security systems/applications such as CCTV, access control and monitoring systems (ACAMS), Identification Management Systems (IDMS), and Perimeter Intrusion Detection Systems (PIDS).

From an enterprise architecture perspective, airport operators since the mid-1990s have been installing high-speed fiber optic networks to support the connectivity and bandwidth required by the variety of operational systems such as building systems, financial systems, passenger processing systems, and security systems. These networks have been supplemented with wireless capabilities supporting a variety of communications protocols. Additionally, a growing number of airports have been implementing robust converged networks using resilient architectures to support the data, voice, and video demands of an airport operational environment.

As the next generation of integration and technology moves ahead, the communication network should be supported by logical data systems architecture based on industry open system standards to allow a variety of applications and systems to easily integrate onto the network utilizing Services Oriented Architecture (SOA) framework, middleware, and Web services technologies. The airport data systems architecture should also be flexible enough to support a variety of data marts, databases and data warehouses at the airport. In terms of security systems design these are critical infrastructure elements that will allow information to be shared among multiple systems at the airport.

Beyond the supporting communications elements, the security elements require reliable and managed power elements. This will include UPS and emergency power at the communication rooms for critical equipment, Power over Ethernet (PoE) for many end devices, and other power solutions depending on location, purpose and type.

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

The communications network supporting security systems should not only have high system availability but also should ensure data integrity and data security. Airport operators should ensure that appropriate network information/data security solutions and protocols are incorporated within its enterprise network architecture not only at the network level but also at the application/session level. Loss of functionality or data integrity on these systems risks jeopardizing the airport's safety and security. While some of the most critical data being transmitted pertains to the airport's access control and monitoring system (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 impact flight operations 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.

The interconnection of these systems is cumulatively referred to as the Information Technology (IT) infrastructure and sometimes as the Premises Distribution System (PDS), although PDS primarily refers to the low voltage cabling, pathway, and network electronics and does not typically include the power elements and enterprise integration platforms. Component portions should be designed and installed to operate seamlessly. The equipment and components of the individual power, communications, and infrastructure systems should be designed, selected, and placed in locations that secure them and provide for reliable operation during an emergency. The design process for the IT infrastructure should examine each design element at the earliest possible stages to ensure a successful supporting infrastructure methodology. Design elements should be applied both internally within the system itself, and externally at each point where systems connect. This will help ensure compatibility, connectivity, and security throughout the design process and into installation and operation.

2. 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 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 separations 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 all airports are not new facilities. Most were built prior to the introduction of contemporary integrated systems; the electric power distribution infrastructure often is not configured to meet current security requirements.

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

If possible, the power source for a building should be from two separate sources, such as an emergency diesel generator system connected to the emergency (bus) distribution system. Use of automatic transfer switches is required to achieve automatic shift to the emergency power source. Electrical system architecture should be evaluated to provide the greatest uptime and availability through the use of 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 percent future growth. Coupled with the use of line-powered CCTV, loss of access control power need not violate the integrity of the terminal security system.

Backup power for lighting is required for life safety systems; many options that are allowed under local building codes raise security considerations.

a. 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.

b. Lighting supplied with integral battery packs are a maintenance item and provide less than full power lumen output on the lamps that they control. Battery packs should be tested on a monthly basis as they have the potential to fail if not properly maintained.

c. 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.

d. Egress lighting level should be 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 and surveillance systems.

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 a 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, including physical security of access portals.

Due to the increasing deployment of Internet Protocol (IP)-based CCTV cameras, Power Over Ethernet (PoE) technology is becoming a readily available power source. PoE is advantageous to deploy in applications where USB is unsuitable and where AC power would be inconvenient, expensive or infeasible to supply. However, even where USB or AC power could be used, PoE has several advantages over Ethernet, including less costly cabling, higher bit rate support, direct injection from standard 48 V DC battery power arrays, and symmetric power distribution.

3. 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 employed over the active infrastructure including Ethernet, Token Ring, ATM, Frame Relay, and others. The implemented networking technology determines which data transmission methods can be 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.

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.

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

2) If security and data transmission media (fiber optic or copper cable) are of the same quality and contain spare capacity, each may provide an alternate route for mission critical applications of the other, i.e., redundant cable paths. Physical cable separation of the security and data network reduces

the risk of compromising security; however, in the event of cable damage in either network in an integrated system, a simple cross connect can restore services more quickly, if only on a temporary basis while more complete repairs are performed.

3) Security measures should be taken to protect cabling. Cables, connections, and equipment should be protected from accidental damage, sabotage and physical wire-tapping. This is usually accomplished by placing security related cabling in conduit or EMT and limiting access to telecommunications rooms, where security related cabling terminates. Where security cabling cannot be run in conduit or EMT, the cable should be routed only in pathways in secured areas of the airport and not in publically accessible areas.

4) Passive infrastructure should be designed in accordance with the most recently published communications industry codes and standards, including BICSI Telecommunications Distribution Methods Manual (TDMM), ANSI/TIA/EIA—568B series, IEEE standards for wired and wireless communications, National Electrical Code (NEC), and local building codes.

5) The design flexibility of cable trays within a facility should also be reviewed as it provides the most cost-effective and high-density pathway for security and data cabling. As requirements and technologies change, flexibility is a key point to consider.

6) A carefully designed and installed signal ground system is critically important to successful operation of digital data equipment

Since CCTV became a fixture at airports, video cameras have often been wired by “home-runs” directly to a Security Operations Center (SOC) over dedicated copper cable, usually coax type, or over fiber optic cable. The selection of cabling should be based on the transmission distances (longer distances favor fiber), security (fiber cables are difficult to tap and are not susceptible to electromagnetic interference), and cost (fiber has been more expensive than copper cabling, but the gap is closing and the bandwidth advantages of fiber are compelling).

The video cables are then terminated in multiplexers or in matrix switches, from which the signals are routed in analog form to monitors and storage devices such as tape recorders, digital video recorders (DVRs), and network storage media.

The cabling model for networked video is quite different. Network requirements rather than video requirements will govern the configuration, and will generally favor connecting cameras as close to the edge of the network as possible rather than home-running the cameras to a central point, especially when more than 100 CCTV cameras are to be networked. When large numbers of cameras are to be networked, having a dedicated network rather than attempting to transmit video over a shared IT infrastructure should be considered.

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 single mode types.

In the United States, 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). These standards define methods 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. 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 provided 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 telecommunications rooms throughout the airport campus. The physical connectivity between components within each of these rooms is achieved through the passive infrastructure.

When designing an active infrastructure to support security, the two primary elements to be considered are reliability and security. The design 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

Design all telecommunication 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, telecommunications rooms should 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 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

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 appropriately restrictive 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 is installed, and standards for labeling, such as color-coding or other identification methods. The cabling management plan should also discuss assignment of cabling for each individual system's use, and a "Conduit Plan" that documents the origination and destination of all conduit runs within the facility. Clearly, this is not merely an early planning function, but should be maintained for all on-going changes throughout the entire life cycle of the system.

Among the issues of cable infrastructure labeling is the determination of whether to identify security cabling/infrastructure as such. This is an airport decision, but should be made in consultation with the 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:

1) Ease of identification reduces maintenance and repair times.

2) Coding can identify cables to authorized maintenance and repair individuals without providing identification to the public or other unauthorized individuals. Cables are seldom in the public view, often hidden they are typically above a dropped ceiling within a plenum space. Sometimes roof mounted raceways and cable trays are used to accomplish connectivity.

3) Color-coding allows system identification without visually identifying the associated access point, communication line, or piece of equipment.

4) Identification is valuable and can reduce costs when expanding, renovating or modifying systems and/or architectural areas. It helps prevent accidental damage or cable cutting by installers and maintainers of adjacent systems.

5) The disadvantages of visually identifying security system passive architecture include:

   a) Use of identification can direct vandals or saboteurs to critical systems more easily.

   b) 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.

6) 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, routing and isolating cabling.

   Cabling management maintains the system and standards by which cabling and cabling infrastructure systems are installed, maintained and labeled both initially and throughout the airport's lifespan.

   With the variety of users and levels of service required at an airport, it is critical to use and maintain a consistent cable documentation system. There are several commercially available programs that track and document the cable infrastructure of facilities. Redundant infrastructure may be added for different users if there is no centralized control of the cabling structure within the facility. As various users, such as LAN systems, concessionaire Point-of-Sale systems, and security equipment, compete for airport cable bandwidth, spare fibers and conduits will be used on a first-come-first-served basis in the absence of centralized, thoughtful management and control.

f. Network Standards

Standards are essential for networks to function properly. There are four main networking standards bodies that should be of interest to airports:

1) In the United States, the Institute of Electrical and Electronic Engineers (IEEE) publishes standards for networking architectures, such as Ethernet networks; for network devices such as a network switch or a wireless access point; and for a variety of electrical power, communications, and other equipment and systems.

2) Also in the U.S, the Internet Engineering Task Force (IETF) publishes standards for protocols and devices which operate over the Internet.

3) In Europe, the main standards bodies are the International Telecommunications Union (ITU) and The International Organization for Standardization (ISO).

Transmission distances permitted over networks cabling vary by type of cable. The applicable IEEE performance standards for Gigabit Ethernet networks are listed in *Table III-I-1*.

Network standards continue to evolve. The IEEE has approved standards for 10 Gigabit Ethernet and, in 2010, approved 40/100 Gigabit Ethernet transmissions which will provide airports with even greater opportunities for networking surveillance video.

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	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

Table III-I-1—IEEE Ethernet Standards and Cable Distances for Gigabit Service

Given the frequency of moves/adds/changes to airport systems as operations change over time, it is important that all video networking be configured, installed, and tested according to recognized standards and consistent administrative protocols.

The common Ethernet architecture calls for three network tiers: the network core, the distribution (or aggregation) layer, and the application (or access) layer. Airports most recently are deploying mostly 10 Gigabit Ethernet equipment at the network cores and 1 Gigabit equipment in the distribution network, and 1 Gigabit or 100 Mbit equipment for applications. LAN-attached devices are connected to access switches, aggregation switches then connect to core routers/switches that provide routing, connectivity to wide-area network services, segmentation and congestion management. The IEEE-803ba Standards working group has approved a 40/100 Gbit/sec.

With the availability of 10 Gigabit and higher bandwidth core equipment, in many cases it will be possible to "flatten" the network by eliminating the distribution (aggregation) layer. For video transmission, this reduces network transmission delays (latency) resulting in improved video transmission across the network. It should also reduce equipment acquisition and maintenance costs.

- The latency inherent in a three-tier approach should be examined when video is a major network payload.
- The emergence of 10 Gigabit Ethernet, and the 40/100 GbE standard approved by the IEEE provides an opportunity to use a 2-tier network architecture which, in addition to reducing latency, will result in fewer switches to install, operate, and manage.

g. Mobile Remote Display Units

The network infrastructure should also support mobile access to video imagery. Airport security response 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 an excellent capability, so that mobile users remain connected to the SOC and are aware of events as they unfold.

h. 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:

1) Dual (or multi-) network cabling to interconnect mission-critical computing equipment and platforms. The dual network cables can be routed along physically diverse paths to minimize the chances of being damaged simultaneously.

2) Redundant network equipment, such as repeaters, switches, routers and power supplies, should also be considered. Separate wiring closets may be allocated to host the redundant equipment (as physical distance limitations allow) and should be placed far enough apart to reduce the chances that all the equipment will be damaged in a single destructive event.

3) The use of Power Distribution Units, 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.)

4) A UPS should be installed at each Intermediate Distribution Facility (IDF) and Main Distribution Facility (MDF) to provide both reliable and clean power to the downstream loads.

5) 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.)

6) Systems such as 400-hz aircraft ground power units and chargers for electric ground service equipment should be isolated and fed from dedicated sources if possible.

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.

Network architecture should include the appropriate "meshed" configuration to provide multiple routes between network components in the event of equipment or cabling failures.

i. 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, airports, concessions, and government organizations.

Many large and medium airports have installed a shared communications network to achieve high Quality of Service levels and high system availability rates, particularly useful if airport operators expect tenants, including airlines and the TSA, to share the network.

In most cases, airports have established a separate "security systems network" physically separate and distinct from the airport network used for the traditional operational systems. With the improvement of communications technologies such as VPNs and network security features, airport operators are now hosting security systems and related applications on the shared airport network.

There are pros and cons of sharing versus not sharing the networks, but those discussions are beyond the purpose of this guideline. It is recommended, however, that all relevant stakeholders (operations, engineering, IT, security, and if applicable, the TSA), agree on their mission and system requirements, and determine which solution is best for its application. This is typically laid out in the initial Concept of Operations.

j. 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 taking into account redundancy and back up. Storage redundancy may be achieved by mirroring storage devices in different locations via local area networks, using Redundant Array of Independent Disks (RAID) techniques, Storage Area Network (SAN) techniques, or Network Attached Storage (NAS) techniques, among others. These strategies require the airport to allocate separate space and infrastructure for redundant equipment. The distance between storage system rooms should be great enough to reduce the chances of all the rooms being damaged during the same event.

k. Network Bandwidth

Usage of digital technologies for CCTV cameras has increased the typical airport network bandwidth requirements, but communications network technologies have improved data rate transmission to where it is very typical for airports to design 10 Gigabit Ethernet networks. In terms of security system design, the requirements for frames per second and frame size (video resolution), and video compression techniques will ultimately determine the bandwidth requirements of the network.

During the design phase it is important for the airport communications network to be sized for “worst case” scenarios in terms of bandwidth. This would be a situation in which multiple airport security and operations personnel would have to make maximum and possibly simultaneous use of the networked equipment, such as examining live and recorded video from multiple cameras. This could easily require 10 to 20 times the normal network capacity needed for security. Unlike business applications which can have easily established activity patterns (in terms of network load), security systems (CCTV/NVRs, etc.) can be moderate until an alarm or security incident occurs, introducing immediate heavy demands on top of continuing normal loads.

As a result, to accurately assess the network bandwidth requirements, a scenario based design approach should be used that examines security system use during various security and business conditions, including a security and/or emergency incident response at the airport.

There are some well-proven techniques for reducing the bandwidth loading on a network, such as positioning the NVRs near (in network terms) the camera clusters; use of Multicast technology; and use of ACF (Activity Controlled Frame rate) at the camera whereby the video transmission rate is adjusted based on scene activity.

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 during an earlier construction job. This helps avoid future need to tear up and repair walls or floors, dig trenches, and pull cable.

5. Radio Frequency (RF)

There are five broad considerations when RF-based communications are introduced to an airport environment:

a. Is RF-based communication the most efficient and cost-effective way to accomplish the necessary tasks?

b. Will RF-based communication require unique infrastructure support not necessary with other modes of communication?

c. Will airport RF systems interfere with other operational elements, including aircraft and air traffic communications, security operations, or general administrative data transfers?

d. Will they operate in all, or at least the necessary portions of the terminal and grounds?

To answer these questions, the designer should consider the sources of RF and the systems that might be affected by targeted or random RF emissions.

a. Environmental Considerations for RF include:

   1) Electromagnetic Environment

      Potential sources of electromagnetic interference with RF include:

      a) Cell Phones

      b) Licensed and unlicensed equipment

      c) Metal detectors

      d) X-Ray machines

      e) Explosive Detection Systems

      f) Advanced Imaging Systems

      g) Portable devices (pagers, PDAs)

      h) Power Generators

      i) Power lines

      j) Power transformers

   2) Physical Environment

      Physical environment can affect RF communications, depending primarily on the frequencies used, and to a lesser extent on the communications protocol. Relevant environmental variables include most weather conditions:

      a) Dust and dirt
      b) Rain
      c) Snow
      d) Temperature

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:

   1) Antenna—Location, mounting, and directional/omni-directional considerations.
   2) ATC communications interactions and interference.

3) Coverage areas (and dead spots).
4) Mobile or portable.
5) Obstructions.
6) Other collocated or local transmitters, including those external to the airport, which have the potential to "interact" with airport RF communications systems.
7) Robustness of link.
8) Shielding.

d. Wireless Systems

The three types of wireless systems that are likely to be useful for airport security are:

1) Radio frequencies which are licensed to the airport by the Federal Communications Commission (FCC).

2) Radio frequencies which the FCC has ruled may be used without a specific license.

3) 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 Wi-Fi 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 when properly prepared, but obtaining a license is never guaranteed.

The FCC has set aside several frequency bands for unlicensed wireless operations. The most popular commercial bands are the Part 15 Subpart C, known as the ISM band (for Industrial-Scientific-Medical users) and the frequencies set aside for wireless local area networks (WLANs), known as the Part 15 WiFi bands. They are power limited to minimize interference, which means limited range, which in turn can be overcome with high gain antennas.

Although the Part 15 WiFi bands are governed by IEEE standards, they are public, which means they can be monitored by anyone within the power/bandwidth envelope or the antenna beam. They can also be saturated with public users; the rated distance assumes a single user. Adding one user could drop the range in half depending on the bandwidth of the transmission, i.e., video vs. text. The only protection from interception is encryption; there is no practical protection from saturation.

Several standards exist, and continue to evolve, but for airport use the most significant are:

- IEEE 802.11a—operating in the 5 GZ band.

- IEEE 802.11b/g — operating in the 2.4 GHz band.

- IEEE 802.11n—range enhancements for operations in the a/g bands.

IEEE 802.11b is the original WiFi band, later expanded under the "g" standard for higher data rates and lower dropped packet rates. 802.11g was the third modulation standard for Wireless LANs. It works in the same 2.4 GHz band as 802.11b, but operates at a maximum raw data rate of 54 Mbit/s, and 802.11g hardware is fully backwards compatible with 802.11b hardware. Higher throughput is achieved by a more efficient modulation scheme, and to reduce susceptibility to interference there are only three non-overlapping usable channels in the United States with 25 MHz separation. Even with such separation, some interference due to side lobes exists, though it is weaker than for "b" signals. This band is also shared by other emitters including Bluetooth devices, cordless telephones, and microwave ovens—all potential sources of interference.

The IEEE 802.11a band improves on the 802.11b/g standards and also provides for operations in an alternative, possibly less congested band. The 802.11a band offers over three times the operating bandwidth over the spectrum available in the 2.4-GHz band with less susceptibility to interference. The modulation scheme of 802.11a has fundamental propagation advantages when in a high multipath environment, such as an indoor office, and the higher frequencies enable the building of smaller antennas with higher RF system gain which mitigate the disadvantage of a higher band of operation.

The IEEE 802.11a band has 12 non-overlapping channels, 8 dedicated to indoor and 4 to point to point applications. The 8 indoor carriers are spaced across 200 MHz in the lower spectrum (5.150–5.350 GHz) and 4 point-to-point carriers are spaced across 100 MHz in the upper spectrum (5.725–5.825 GHz). The channels are spaced 20 MHz apart, which allows for high bit rates per channel. Maximum raw data rate in this band is 54 Mbit/s, which yields realistic net achievable throughput in the mid-20 Mbit/s. The effective overall range of 802.11a is slightly less than that of 802.11b/g because 5 GHz signals are absorbed more readily by walls and other solid objects in their path.

To provide still higher throughput in wireless LANs, the IEEE developed 802.11n which enhances operations in the 802.11a/g bands. The throughput can exceed 100M bit/sec in 20-MHz to 40-MHz of bandwidth and enables interconnection distances of 300 feet or more. The increased performance is achieved by using multiple antennas, known as multiple-input/multiple-output or MIMO technology, to coherently resolve data streams in the presence of signal multi-pathing. The 802.11n technology also aggregates packets so the data is sent in longer units, decreasing the overhead of the packet preambles, and uses spatial division multiplexing (SDM) which multiplexes multiple independent data streams simultaneously within one spectral channel of bandwidth. Many applications, and particularly streaming video such as the output of surveillance cameras, can require throughputs of 100M bit/sec and higher. The 802.11n also increases channel bandwidth to 40 MHz, doubling the channel width (and data rate) from 20 MHz in the 802.11a/g bands.

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 802.11a band solely for airport use this problem can be mitigated.

Optical wireless systems use laser beams to carry video and other information. These are usually point-to-point systems. An optical beam is very narrow and cannot be detected, or captured, by radio receivers. Optical wireless systems also generally transmit in the infrared band, so the beams are not visible to the naked eye. These features make optical wireless difficult to intercept and attractive for secure transmissions.

On the other hand, the reliability of optical beams depends on the quality of the atmosphere. Rain, snow, fog, and sandstorms can degrade a link or even cause it to fail. This is a function of the link margin, i.e., the power of the received beam over the transmitted distance compared to atmospheric losses. For many environments, at the level of service required for security systems (equal to the telecommunications service level of 99.999 percent), optical transmission links are only candidates for relatively short distances. If there is uncertainty about the optical link performance, it should be tested under the local environmental conditions of worst-case concern before a commitment is made to use such equipment.

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 stance that it alone can regulate radio operations.

Airport operators can seek to limit interference through voluntary agreements with tenants, who face the same problems, and can also restrict tenants from attaching Wi-Fi antennas to airport property, but under existing FCC rulings airports cannot otherwise prohibit a tenant from operating Wi-Fi equipment.

e. Considerations Related to the Use of Radio Frequency ID Devices

Radio Frequency Identification (RFID) tags and other RFID equipment are entering use in the airport security system. In some airports, RFID is already used to track selected bags in the inspection process, and in air cargo. Standards for RFID tags are not mature at the time of this writing. One standard would use RF frequencies in the 13.56 MHz range; another in the 2.45Ghz range. The latter range is available for unlicensed use within the United States and is currently the frequency range of choice for a number of commercial 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 an 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; hence their radiation emission and susceptibility can be better predicted and controlled. Also, the RF environment outside of a physical building is much more unpredictable, so efforts should always be taken to "isolate" as much as possible the internal and external environments.

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.

6. Information Assurance for Airport 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.

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.

7. Cyber-Security of Airport Networks

The aviation industry, airports in particular, are highly dependent on information technology (IT) for their daily security operations. These IT systems are widely used as the platforms for airport access control and alarm monitoring systems, CCTV camera systems, plus other command, control, and dispatch systems. These functions allow for increased capabilities, long term cost savings, and in many cases, the IT systems act as force multipliers, allowing the airport to perform and monitor more functions with fewer employees.

With this increased capability and ultimately an increased dependency, comes an increased risk of exposure to cyber attacks. In addition, because of the need to protect proprietary information, and personally identifiable information of passengers and employees, airports have a need for securing all of these differing IT systems. Also important to note, some terrorist acts are organized and facilitated using the Internet and connected IT systems, using the same IT infrastructure used by airport operators. Therefore, planning for the physical security of these airport IT systems, designing these robust systems with multi layered protection, and combining these with restrictive user policies are a good start in protecting these critical systems from cyber attack.

Unauthorized access to communication and data networks can take many forms:

a. Authorized individuals failing to log off or re-secure their access points or computers, making available undetectable unauthorized access by others.

b. Authorized individuals gaining access to portions of the network they are not authorized to access.

c. 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, which in turn suggests a need for strong password protocols.

d. Unauthorized individuals gaining access to the network from computers or systems on premises that normally do not allow access.

e. Unauthorized individuals gaining net access through external connections such as modems or wire-taps.

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

a. Administrative Control. The security system applications and network shall support the airport's own security standards, policy and procedures, including password policy.

b. Logical Control. Use software and data to monitor and control access to information and computing systems, e.g., passwords, network and host based firewalls, network intrusion systems, access control lists, and data encryption techniques.

c. Physical Control. Monitor and control the telecommunications rooms where equipment and infrastructure is located. Use access control systems to secured areas critical to the airport network.

8. Physical Security of Critical IT Systems

a. Location and facility design—Critical IT systems should not be housed in areas with public access. They should reside in places where security oversight is readily available. They should also be designed to withstand moderate exterior explosions.

b. Environmental Controls—Critical IT systems should be housed in spaces that can independently compensate for drastic changes in temperature, moisture and pressure. They should also have back-up power to allow safe shutdown in the event of loss of power or climate control systems.

c. Mechanical, electronic and procedural access control—IT systems should be housed in spaces that employ electronic and physical access controls to deter tampering or disabling of the system. These can include ID badge systems, combination pads, locks or manual locks, and/or key systems with proper accountability.

d. Intrusion Detection—Intrusion detection systems may also be employed in these spaces to add an extra layer of security. The intrusion detection should be actively monitored and procedures should be in place in event of compromise.

e. Video Monitoring—It is advisable to use CCTV or other video monitoring, ideally on isolated networks, inside the spaces housing critical IT systems to deter the tampering or disabling of the system.

f. Remote Redundancy—Whenever location and budget allow, avoid single points of failure in critical IT Systems. One method is to incorporate a secondary or redundant system in parallel with the primary system. This should be part of an extensive continuity of operations plan to allow continued operations in the event of loss of primary systems.

9. Designing Security for the IT Systems

In designing an IT system, the system's operational requirements (including information security requirements) should be identified first. It is important, whenever selecting systems that security is built in rather than added later. The system should be designed and built to meet both operational and security requirements. The more complex an airport IT system is the likelihood of "missing something" exists, thus opening up a potential vulnerability. Many modern airport IT networks link multiple critical systems which are then supplied with data from several external sources, which can bring their own vulnerabilities. For this reason, it is critical that the airport IT planner/designer ensures that each connection is secure, protected by the appropriate firewalls, and that the data transmitted is appropriately encrypted. Communication between the sharers of information is critical in minimizing the weak links in the process. *Figure III-I-1* is a diagram of a typical computer network with Internet access.

The five contributing factors to the escalation of cyber attacks in recent years:

a. Utilization of standardized technologies with known vulnerabilities.

   IT systems connected to other networks that are not secure, thus exacerbating vulnerabilities.

b. Insufficient or misconfigured firewall protection.

c. Lack of or weak encryption of data traversing the network.

d. Lack of an effective user awareness program, to include policies, procedures and technologies.

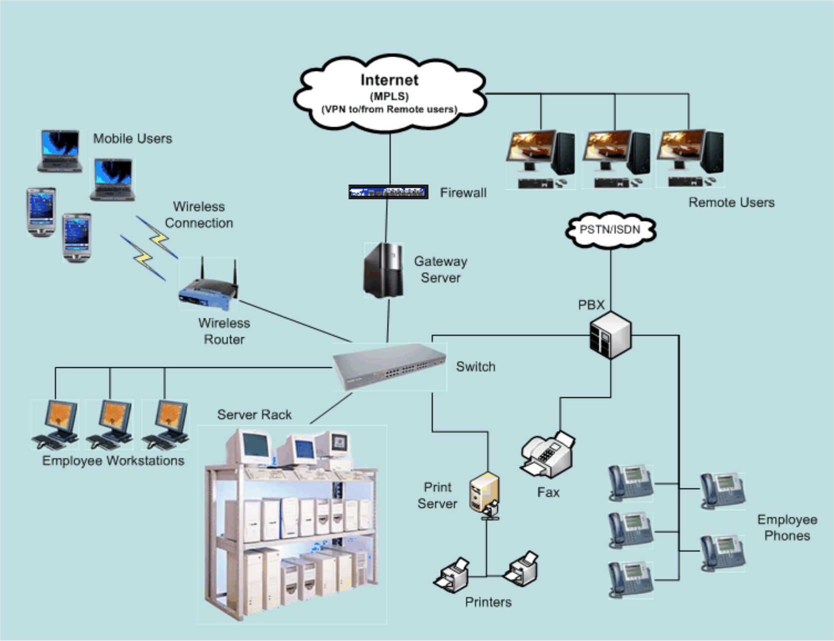


Figure III-I-1—Typical Network with Internet Access

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

10. Cyber Security & Risk Management

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

a. Security Policy

   Describe the organization's information protection objectives as stated by management.

b. Security Awareness

   Implement activities to ensure that every individual is made aware of their security roles and responsibilities.

c. Security Architecture

   Create a structural blueprint of the technology and processes that will be employed to accomplish the goals of the security policy.

d. System Prioritization

   Develop a ranked inventory that identifies the organization's critical systems and sensitive data.

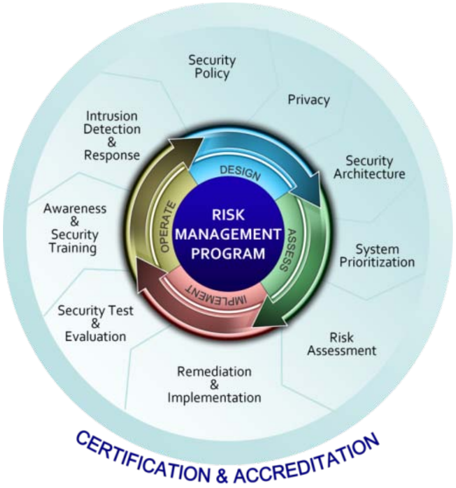

Security Policy
Privacy
Security Architecture
System Prioritization
Risk Assessment
Remediation & Implementation
Security Test & Evaluation
Awareness & Security Training
Intrusion Detection & Response
DESIGN
ASSESS
IMPLEMENT
OPERATE
RISK MANAGEMENT PROGRAM
CERTIFICATION & ACCREDITATION

Figure III-I-2—Recurrent Steps of Cyber-Risk Management Cycle

e. Risk Assessment

Conduct a threat/vulnerability/consequence/risk analysis that determines the effectiveness of existing security countermeasures.

f. Remediation and Implementation

Develop a plan for mitigating each residual risk to an acceptable level.

g. Security Test & Evaluation

Perform an in-depth validation of the systems security countermeasures.

h. Security Training

Provide periodic information and training for individuals responsible for implementing the organization’s security countermeasures.

i. Intrusion Detection and Incident Response

Implement procedures to gather and analyze information to identify potential unauthorized access and steps to take when detected.

NIST Risk Management Framework (RMF): The NIST Risk Management Framework (RMF) and NIST 800-53 “controls” can be applied by airport IT staff. Measures at airports of different sizes and complexities will have different security risks and mitigation requirements.

Section III-B—IT, Power, Communications & Cabling Infrastructure Systems Checklist:

□ **Operational Requirements from ConOps**

□ **Secure emergency operation**

□ **Power**

- Low voltage devices and controls
- Battery remote and stand-alone devices
- 110/220 VAC for lighting, CCTV
- High amperage systems for X-rays, EDS
- Capacity of stand-by generators
- Redundant power lines to all locations
- Conduit pull-strings for future work

□ **Cabling Infrastructure Systems & Management**

- Cabling Management

    - Standards for cable type/location
    - Labeling, color-coding for ID

☐ **Security of Airport Networks**

- Network Availability Considerations
    - Multi-net cables—critical systems
    - Different paths to minimize damage
    - Redundant repeaters and separate closets for switches, routers, power
- Network Security
    - Protect from unauthorized access
    - Encryption for general network
    - Shared vs. dedicated fiber is a design/cost issue
- Network Accessibility
    - WAN connectivity—Internet/or VPN
    - Shared network security issues
- Information Storage Availability
    - Storage reliability: server/database
    - Storage redundancy and back up
    - Separation of redundant equipment
    - Distance between storage rooms

☐ **Future Rough-Ins/Preparations**

- Early planning reduces future costs
- Expansion includes extra conduit, cable.

☐ **Telecom Rooms**

- Short direct lines to each other
- Working space for expansion
    - power, cooling, fire, dust control

☐ **Radio Frequency (RF)**

    - Consider efficiency and cost
    - Potential interference with other operational elements

☐ **Physical Environment Concerns**

- Temperature
- Rain & snow
- Dust and dirt
- Regulations—Coord./w FCC, FAA, and TSA

☐ **Installation Considerations**

- Antenna location, mounts, direction
- Potential interactions w/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” RF environment is not predictable, need internal “isolation.”
- Choke Effects Integral to Construction
    - Low frequency/long wavelengths can “match” terminal openings
    - Subsurface metal rods, I-beams at openings can create RF choke
- Other Lessons Learned
    - Electrical & electronic environment at airports rarely remains constant
    - There is always more that can be done to improve the EMC status
    - Loading bridge orientation can reduce unwanted radiation

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

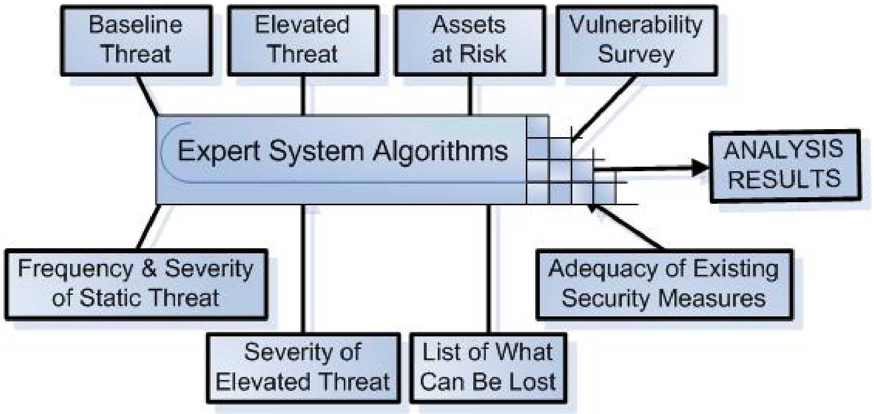
Section A—The Vulnerability Assessment

The 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 than as a more expensive retrofit. Vulnerability is the susceptibility of the airport 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.

Threats are defined as specific activities that will damage the airport, its facilities, or its 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 threat and vulnerabilities must not only measure the degree of potential danger, but the chances of that particular danger actually occurring.

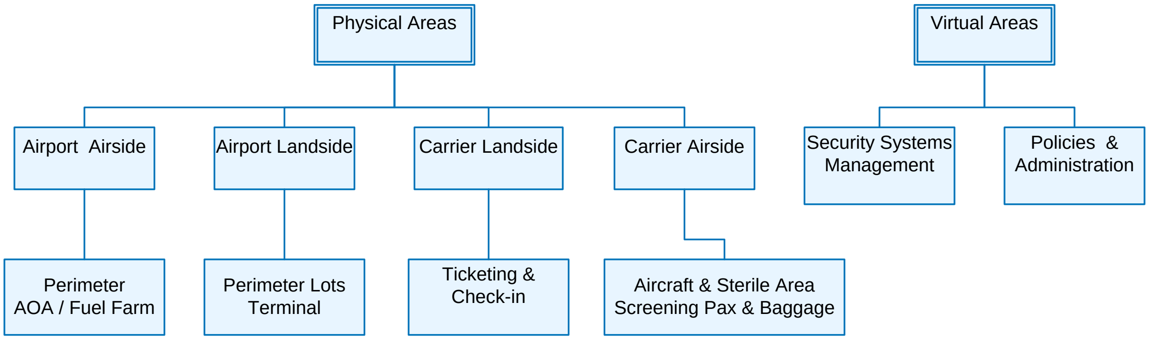
Threats and vulnerabilities cover a wide array of events, virtually none of which can be totally eliminated while still operating the system. Since no system can be rendered totally secure, once threats and vulnerabilities are identified, their impact on the total system must be assessed to determine 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 continuing process of risk management, identifying major threats, and considering how vulnerable the system might be to the actions they threaten.

Some factors to consider in assessing vulnerabilities, quantifying risk and allocating resources include: baseline threat, elevated threat, assets, vulnerability surveys, the frequency and severity of the static threat, the severity of the elevated threat, an inventory of what can be lost, the adequacy of existing security measures, and the ability to recover from the consequences of an event. 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. *Figure A-1* is an example of an assessment model.



Appendix A Figure A-1—Assessment Model

The TSA offers airport operators the Commercial Airport Resource Allocation Tool (CARAT), which is available to airport operators governed by 49 CFR Part 1542 on TSA's secured Web board. This tool enables the user to assess and compare the cost-effectiveness of security measures across scenarios. The CARAT is sensitive security information and should be handled accordingly.



Appendix A Figure A-2—Model for Assessing Vulnerabilities

TSA's Office of Security Assessments, which is under the Office of Law Enforcement, conducts Joint Vulnerability Assessments (JVA). The JVA is a joint effort undertaken by the TSA and the Federal Bureau of Investigation (FBI) with the purpose of assessing current and potential threats to commercial air transportation facilities within the United States. The process is a direct result of the increasing threats to aviation which prompted Congress to pass Section 310 of the Federal Aviation Reauthorization Act of 1996 requiring the Federal Aviation Administration (FAA) and the FBI to conduct joint threat and vulnerability assessments of security at United States' airports. In response to this mandate, during fiscal years 1999, 2000, and 2001, the FAA and FBI prepared three-part assessments addressing the vulnerability, criminal activity, and terrorist threat at selected airports nationwide.

In FY 2002, the TSA acquired responsibility for the assessments from the FAA through the Aviation Transportation Security Act (ATSA). In addition to the JVA, the TSA Office of Law Enforcement also conducts Man Portable Air Defense System Vulnerability Assessments (MANPADS). MANPADS Vulnerability Assessments are conducted to help identify and define potential launch locations in areas surrounding the airport by using known terrorist methodology and weapon employment tactics and capabilities. While potential launch areas vary, they are all subjected and graded by utilizing seven specific characteristics. This multi-dimensional program is designed to deter, detect, mitigate, and defeat the MANPADS threat. TSA conducts MANPADS Assessments while working closely with local law enforcement officials in developing and coordinating mitigation efforts.

The TSA Office of Security Assessments conducts JVAs and MVAs at specific airports, both by mandate and upon request by the airport operator. To request a JVA or MVA the airport operator should contact the local Federal Security Director (FSD) to make the request.

TSA is currently determining the most effective way to evaluate airport vulnerabilities based on threat assessments. Airport vulnerability assessments may also 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 may include analyses conducted by appropriate law enforcement agencies (Federal, State and local) in conjunction with the local airport operator, 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 operator, 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.

In addition, TSA has compiled a compendium report which includes detailed information collected from airport operators about security initiatives currently in use at commercial airports and widely regarded as innovative security measures; it is available through the TSA Web board or the local FSD. Another tool available for use from the TSA is the Airport Security Self Evaluation Tool (ASSET), which allows individual airport operators to conduct risk assessments.

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.

Most assessment tools, such as the TSA's CARAT, are subjective. They need to take into account local threat considerations and operators' perceptions of the effectiveness of current or proposed security measures in reducing vulnerabilities within the unique operational environments of their particular airports.

The threat and vulnerability assessment process for a transportation system is conceptually diagrammed in Appendix A Figure B-1 for a transportation system. Assessments typically use a combination of quantitative and qualitative techniques to identify security requirements, including the historical analyses of past events, intelligence assessments, physical surveys, and expert evaluation. When the risk of hostile acts is greater, these 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.

Effective assessments typically include five elements, each of which will be discussed in this section:

- Asset analysis;
- Target or threat identification;
- Vulnerability assessment;
- Consequence analysis (scenarios); and
- Counter-measure 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 operator may wish to consider:

   - The value of the asset, including current and replacement value;
   - The value of the asset to a potential adversary;
   - Where the asset is located and how, when, and by whom an asset is accessed and used; and
   - What is the impact, if these assets are lost, on passengers, employees, public safety organizations, the general public and airport operations.

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 capability, intent, motivation, and possible tactics of those who may carry them out.

The process involves gathering historical data about hostile events and evaluating which information is relevant in assessing the threats against the facility.

Some of the questions to be answered in a threat analysis 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*. Historical examples are provided for reference and consideration, as well as to illustrate the types of weapons typically used in these attacks.

Type of Attack	Historical Examples	Type of Weapons
Explosive and Incendiary Devices	2011—Attack on Domodedovo Airport, Moscow, Russia	Suicide bomb; Incendiary device
	2009—Attempt to detonate device on-board Northwest Airlines Flight 253	Concealed body-worn plastic explosives
	2010—Hidden explosives in cylinder of thermal liquid containers at screening checkpoint	Improvised explosive device
	2010—Discovery of explosive devices hidden in printer toner cartridges on all-cargo flights from Yemen	Improvised explosive device
	2010—Incendiary devices mailed to Maryland and Washington DC area facilities	Incendiary device
	2007—Attack on Glasgow International Airport	Incendiary device
	2001—Attempt to detonate device on-board American Airlines Flight 93	Concealed body-worn plastic explosive
	2001—World Trade Center 1995—Oklahoma City bombing	Proximity bombs, incendiary & secondary devices,
Stand-Off Attack	2001—Tamil Tiger mortar attack and bombing of Sri Lanka's national Airport	Anti-tank rockets, mortars
Cyber Attack	2002—Code Red Worm	Worms, Viruses, Denial of Service Programs
Chem-Bio, Radiological, & Nuclear (CBRN)	1995—Aum Shinrikyo Sarin agent release in Tokyo Subway	Chemical, biological, or radiological or nuclear aerosolized

Appendix A Table B-1—Examples of Terrorist Attacks and Weapons

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. Consequence Analysis (Scenarios)

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 performed to recognize, prevent, and mitigate the consequences of attacks. *Appendix A Table B-2* lists examples of likely threats to airports.

Assets	Most Probable Threats
Terminals	o High Yield vehicle bomb near terminal o Low yield explosive device in terminals o Hi-jacking, hostage or barricade situation in terminal o Chemical, biological or nuclear release in terminal o Secondary explosive directed at emergency responders
Fuel Storage Facilities	o Explosives detonated in/near fuel facilities
Security Operations Centers	o Physical or cyber-attack on dispatch system o Armed assault, hostage or barricade situation o Explosive device in/near Operations Control Center o Sabotage of vehicle or maintenance facility

Appendix A Table B-2—Examples of Likely Threat Scenarios

The FBI recommends that transportation systems focus on the top 10 percent 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 operator should also consider the range of perpetrators, such as political terrorists, radicals, right-wing extremists, disgruntled employees, disturbed copycats, and others.

When conducting the scenario analysis, the system may choose to create chronological scenarios (event horizons) that emphasize the worst credible scenario as opposed to the worst case scenario.

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.

<table>
<tr><th>Vulnerability of Target</th><th colspan="2">Impact</th><th>Criticality Matrix</th></tr>
<tr><td>A
Very easy</td><td>I</td><td>Loss of Life</td><td rowspan="5">
<table>
<tr><td colspan="5">H=High S=Serious L-Low</td></tr>
<tr><td></td><td>I</td><td>II</td><td>III</td><td>IV</td></tr>
<tr><td>A</td><td>H</td><td>H</td><td>S</td><td>S</td></tr>
<tr><td>B</td><td>H</td><td>H</td><td>S</td><td>L</td></tr>
<tr><td>C</td><td>H</td><td>S</td><td>L</td><td>L</td></tr>
<tr><td>D</td><td>S</td><td>L</td><td>L</td><td>L</td></tr>
<tr><td>E</td><td>S</td><td>L</td><td>L</td><td>L</td></tr>
</table>
</td></tr>
<tr><td>B
Somewhat Easy</td><td>II</td><td>Serious injury, major service impact</td></tr>
<tr><td>C
Difficult</td><td>III</td><td>Minor injury, minor service impact</td></tr>
<tr><td>D
Very Difficult</td><td>IV</td><td>No injury, no service impact</td></tr>
<tr><td>E
Too Difficult</td><td>--</td><td>---</td></tr>
</table>

Appendix A Figure B-1—Scenario Evaluation Criteria

Consequences are assessed both in terms of severity of impact and probability of loss for a given threat scenario. *Appendix A Figure B-1* shows one process for accomplishing this.

Scenario-based analysis is not an exact science but rather an illustrative tool demonstrating potential consequences associated with low-probability to high-impact events. To determine the system's actual need for additional countermeasures, and to provide the rationale for allocating resources to these countermeasures, the scenarios can be used to pinpoint the vulnerable elements of the critical assets and make evaluations concerning the adequacy of current levels of protection. Scenarios with vulnerabilities identified as high may require further investigation.

Examples of vulnerabilities that may be identified from scenario-based analysis include the following:

- Accessibility of surrounding terrain and adjacent structures to unauthorized access (both human and vehicular);
- Site layout and elements, including perimeter and parking that discourage access control, support forced or covert entry, and support strategic placement of explosives for maximum damage;
- Location and access to incoming utilities (easy access for offenders);
- 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 operator should have assembled a list of prioritized vulnerabilities for its top 10 percent critical assets. These vulnerabilities may be organized into the following categories, which should be documented in a confidential report:

- Lack of planning;
- Lack of coordination with local emergency responders;
- Lack of training and exercising; and
- Lack of physical security (access control, surveillance; blast mitigation, or chemical, biological, or radioactive agent protection).

5. Developing Countermeasures

Based on the results of the scenario analysis, the airport operator can identify countermeasures to reduce vulnerabilities.

Effective countermeasures typically integrate mutually supporting elements.

- Physical protective measures designed to reduce system asset vulnerability to explosives, ballistics attacks, cyber attacks, and the release of chemical, biological, radiological, or nuclear (CBRN) agents.
- Procedural security measures, including procedures to detect and mitigate an act of terrorism or extreme violence and those employed in response to an incident that does occur.

In identifying these measures, the airport should be able to answer the following questions.

- What different countermeasures are available to protect an asset?
- What is the varying cost and effectiveness of alternative measures?

In many cases, there is a point beyond which adding countermeasures will raise costs without appreciably enhancing the protection afforded.

One countermeasure strategy is to place the most vulnerable assets within concentric levels of increasingly stringent security measures. For example, an airport’s Security Operations Center 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.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

AIRPORT CHEM/BIO PROTECTION AND RESPONSE

A chemical or biological attack on a passenger terminal or supporting infrastructure is a rare event, but potentially significant threat. There are numerous approaches an attacker can take, some of which can be mitigated through HVAC design and other good physical security and procedures. Event management, mitigation and recovery from such an attack will be similar to that from most other airport emergencies, with a few unique considerations. Educating the management and response teams before a chem/bio incident occurs is critical, as is adopting procedures specific to this type of threat

A chem/bio attack against the passenger terminal can come in many forms. The chemical agent could be a gaseous toxic industrial chemical, a less volatile liquid chemical agent, a non-contagious biological agent or a contagious disease. Release of persistent chemical agents or biological materials can require extensive decontamination procedures which could close the facility for up to a year. Any chem/bio agents could effectively be introduced into and disseminated by the terminal HVAC system as a gas or an aerosol of small solid particles or liquid droplets. Other methods of dissemination would call for more direct terrorist involvement, such as distributing a powder to be spread by passenger traffic, or releasing a gas. Explosive dissemination in the public area is also possible, but that removes the covert delayed effect of a chem/bio attack. Approaches to eliminate or reduce the effectiveness of a chem/bio attack follow.

Information in this appendix is in part from “Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism,” by Sandia Berkley National Laboratory.

1. Prevent

   A chem/bio attack will cause significant publicity and may result in extended closure of the facility while decontamination takes place. A loss of public confidence in air travel in general, and in the contaminated airport in particular would likely follow. For this reason, pre-attack hardening of the facility, if it is economically feasible during initial construction or retrofit, is highly recommended. By reducing or eliminating a terrorist’s access to effective chem/bio agent dissemination points using the HVAC system, he will be driven to another target or a less effective approach.

   a. Prevent access to building air intakes and HVAC mechanical rooms

      All building air intakes and HVAC mechanical rooms should be inaccessible to the general public as well as to unauthorized personnel, including airport employees not involved with the HVAC systems. This can be accomplished by using access control systems, intrusion alarms, and security cameras, etc., in addition to physical barriers, physical placement or elevation (placing condensers and high power fans on rooftops).

   b. Prevent access to building structural information (e.g., HVAC blueprints, etc.)

      Building information can allow terrorists to maximize the effectiveness of their attack. Retrieve blueprints and plans from contractors when feasible. Consider marking blueprints as protected information or need to know information. Consider creating a cover sheet to accompany the dissemination of this type of information which provides instruction on information sharing, protection of information and proper dissemination.

2. Detect

   Understanding that an airport has been attacked by a chemical or biological agent is difficult because fast effective sensors with low false alarms are not currently available for the broad range of agents associated with this type of threat. Fast-acting point or line sensors are available for toxic industrial chemicals and volatile chemical warfare agents. Real time biological detectors are not widely available and tend to have excessive false alarm from natural non- hazardous biological materials. The best chemical detectors may be the employees and passengers themselves who are in the terminal and who can often sense a toxic chemical presence and take immediate action. There may be false alarms caused by spills of cleaning products, discarded leaking pepper spray containers, or unacceptable materials collected at the screening checkpoint.

a. Train airport employees to recognize and respond to chem/bio attacks

Training should include an annual drill, and should cover recognition of 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" of potential victims via passenger manifests.

b. 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.

c. 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.

3. Mitigate

The preparation and immediate actions taken by airport personnel will significantly reduce the number of casualties and the extent of facility contamination. Clear procedures for notification and decision-making are essential as time is critical when people are exposed to toxic chemicals.

a. Install and maintain highly effective HVAC filters

Filters should meet or exceed the American Society of Heating, Refrigerating and Air-Conditioning Engineers (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 cannot seep around the filters rather than pass through them). This will provide some mitigation for biological materials.

b. 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 regularly to make sure they respond to remote commands.

c. 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.

d. Establish procedures to analyze contamination and decontaminate exposed people.

Perform decontamination planning and training with airport police, airport firefighters, local hazardous materials and medical teams, and establish procedures for sampling and testing potential chem/bio agents.

e. Create airflow isolation areas to reduce spread of contamination between buildings or zones

1) 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, pressure-balance the HVAC system to minimize air flows between isolation zones (which may consist of entire buildings).

3) Install fire doors or other air barriers that can be triggered remotely in the event of a chemical or biological event.

f. 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 will help protect the staff controlling the emergency response, but will not directly protect the public at large.

2) Air handling units that serve critical areas (such as the SOC) should not provide air that is mixed with re-circulated air from public areas.

g. Establish procedures to “shelter in place” during an outdoor attack or a local industrial accident involving the release of toxic industrial chemicals. Assign responsibilities to close interior and exterior doors; create a chain of command for shutting off HVAC and closing dampers.

h. Pre-identify areas where people can be quarantined and can be segregated by likely exposure (none/unknown/possible/exposed). Assign responsibilities and procedures for rapidly moving people out of contaminated areas without bringing them in contact with unexposed people.

i. Manage other potential chem/bio terminal or crisis management access points

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.

THIS PAGE INTENTIONALLY LEFT BLANK

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 it 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 which have affected how airports operate during heightened threat levels and have impacted airport revenues. 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 can be readily adapted to changing rules and threats. Furthermore, it is prudent to consider the impacts, both financial and operational, of having to cope with the restrictions imposed during high threat levels that occur often or for extend durations. These impacts should not be taken lightly. Airports that are ill-equipped to operate during high threat levels oftentimes face large vehicular traffic backups and long lines at passenger screening portals, both of which add considerable time to a passenger’s point-to-point commute, and affect the airport’s ability to deal with larger, longer-term crowds.

1. Why Airports?

   There are countless potential terrorist targets ranging from commercial buildings to specific social, religious, and political groups. Transportation facilities such as airports, subways, train stations, and bus stations are all potential targets of terrorism not only because they are vital to a stable economy and to the operation of countless businesses, but they are very visible, high-profile facilities filled with a high density of people.

2. Risk Management

   Protection/mitigation from IED and LVIED threats can be provided in many forms:

   a. Security design: using cameras, sensors, alarms, K-9, and patrols, etc.;

   b. Standoff: separation between a potential bomb source and certain targets;

   c. Physical protection: using gates, barriers, blast-hardened columns, blast debris screens, and blast-resistant windows, etc.;

   d. Risk acceptance: through prioritization of protective measures based upon a vulnerability assessment, implementation cost, and overall airport security plan; and

   e. Blend of all of the above: in an integrated security plan that combines mobile security, standoff, physical protection, and risk acceptance into an overall solution.

   While it is important to consider how to provide some measure of blast protection at airports, it is also important to recognize that it is not feasible or cost-effective to fully mitigate all potential 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 on high speed interstate highways, some amount of “risk acceptance” is necessary. Likewise, while it is physically possible to design an airport more like a bomb shelter or fortress, this would severely compromise airport operations, cost substantial amounts of money, and be unacceptable to the traveling public. Each airport operator is left with making important and locally unique decisions on how best to provide reasonable and prudent security and effective blast protection while weighing the effectiveness, cost, and impact on airport operations.

3. Planning Facility Blast Protection

   Security planning should be an integral and early part of all projects undertaken at an airport. Security planning should include performing periodic vulnerability assessments of all facilities and the airport site, as well as evaluating the airport security program to confirm that Federal, State, and local standards have been met.

   At first glance, many blast protection measures seem to focus on protecting airport facilities, such as the terminal building, from the devastating effects of a bomb blast. However, the real priority is to protect the passengers and personnel at airports. Providing blast protection for the facility is simply a means to saving lives in the event that a bombing occurs. Loss of life due to a terrorist bombing reduces significantly if the building remains standing and does not collapse.

   A high level of security is achieved when the airport layout and terminal design complement the airport security plan. Having airport roadways, parking, and terminals positioned and designed with security in mind allows the airport to operate safely and effectively—even during high threat levels. Furthermore, incorporating blast resistant features during the initial design costs less and blends with the overall building architecture much better than costly retrofit of a facility after the fact.

Section B—Common Airport Blast Protection Issues

The following is a summary of common vulnerability issues and recommended methods to physically harden airport facilities. The suggested security enhancements are voluntary upgrade options for an airport to consider. One must recognize that it is impossible to protect everyone from every conceivable threat. This is especially true when protecting public facilities, such as airports, that regularly allow thousands of people and vehicles that have not been screened for weapons or explosives to be in or near the facilities. However, with some planning, one can identify vulnerable areas and prioritize options to mitigate those threats.

1. Level of Blast Protection

   In general, the objective for protecting airports is to provide a “medium” level of blast protection, recognizing that a significant degree of damage to a facility might occur, but the structure will be reusable and remain standing after most conceivable blasts. Some casualties likely will occur, assets probably will be damaged, and some building elements other than major structural members may require replacement.

   In general, it is recommended to implement those security enhancements that protect the primary structure (beams and columns) from catastrophic damage first. All other enhancements are secondary to this. As an example, hardening the windows at a terminal perimeter offers little to no protection if the adjoining columns are destroyed from the bomb blast.

2. Common Vulnerabilities

   a. Roadways

      1) The roadways that surround airport terminals are designed to allow convenient passenger access. However, passenger convenience is often contrary to good security planning. Vehicles that enter airport “landside” property typically are not usually inspected, weighed, or screened except during high threat levels. Restricting or monitoring vehicles that enter landside areas of the airport can be accomplished some distance from the terminal building. Many security guidelines recommend that vehicle barriers be installed that will stop the threat vehicle at locations far enough from the facility to prevent catastrophic damage and minimize loss of life.

      2) Many airports have multi-level roadways (refer to *Appendix C Figure B-1*) that are not physically protected from vehicular attacks or bomb blasts. Airports should consider hardening these columns to prevent severe damage due to vehicular impact or LVIED attacks.

      3) 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*).

Appendix C Figure B-1

Elevated Roadway

Appendix C Figure B-2

Curbside Drop-Off at Ticketing Level

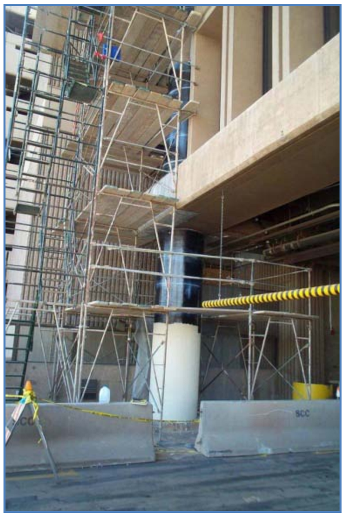
Appendix C Figure B-3

Curbside Pickup at Baggage Claim Level

b. Terminal Perimeter

1) Most exterior windows and doors are not designed to resist bomb blasts. Many security design guidelines recommend that exterior window systems (glazing, frames, anchorage to supporting walls, etc.) be hardened to mitigate the potentially lethal effects of flying glass following a small explosion. However, unlike other secure facilities, hardening the glazing at airport facilities offers limited protection against bombers that are able to flank around the hardened façade simply by walking through the entry doors with unscreened luggage in tow.

2) 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* for an example of column hardening by wrapping process.



Appendix C Figure B-4

Wrapping Process—Kevlar-Carbon Fiber Wrap

3) Many large vehicles can gain uninspected access to terminal properties on either the landside or airside. These include delivery trucks, refuse trucks, construction trucks, and fuel trucks. Several thousand pounds of explosive material can be secreted in these vehicles, and since they are very difficult to visually inspect, they have relatively open access to deliver their bulk threat to any part of an airport.

4) The exterior terminal doors often are not protected from vehicular attack.

5) Exterior trash containers and mail receptacles often are not explosion resistant. Receptacles should not be attached to columns or constructed of materials that would become dangerous shrapnel if a bomb is discharged within the container. 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-5—Potential Concealment Area at Ticketing Level

6) There often are areas at curbside, such as luggage check-in counters and kiosks that could conceal explosive devices (refer to *Appendix C Figure B-7*). 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.

c. Terminal Landside

1) Passenger baggage presents a common challenge in an airport environment. It affords a potential bomber the opportunity to carry up to 75 pounds or more of explosives inside a terminal without much scrutiny—especially in terminals that service international flights, where passengers consistently travel with oversized luggage. In addition, baggage claim areas offer a prime target of opportunity in airports where the area does not have controlled access. Uninspected baggage can be easily introduced in these environments, where it can remain until large crowds gather from an incoming flight.

2) 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.

3) Loading docks and shipping/receiving areas are not often designed to resist bomb blasts. Some security guidelines recommend that loading docks and shipping/receiving areas be at least 50 feet from utility rooms, utility mains, and service entrances such as electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc. Furthermore, when loading docks are located such that vehicles are driven or parked under the building (refer to *Appendix C Figure B-8*), the airport operator should consider hardening the area to resist bomb blasts, and the room should be "vented" outward.

Appendix C Figure B-6—Loading Dock

4) While it is convenient for passengers, the location of parking areas adjacent to the terminal area is not a preferred location from a blast-protection perspective. A blast analysis should be performed to justify parking within 300 feet of the terminal during elevated threat levels.

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. (Refer to *Appendix C Figure B-9*.)

(a) Adjacent Parking Lot **(b) Adjacent Roadway**

Appendix C Figure B-7—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*) as essential facilities. Obviously, the airport must have a fully functional ATCT in order to operate. Public parking adjacent to an ATCT may be limited by FAA regulations. Methods to protect the ATCT structure and cab from blast and ballistic attack also should be considered.

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, fire sprinkler, and water supply
- Fuel storage and fuel delivery systems
- Main switchgear
- Telephone distribution/ main switchgear
- Fire pumps
- Building security control centers
- UPS systems for critical functions
- Main refrigeration systems
- Elevator machinery and controls
- Shafts for stairs, elevators, and utilities
- Critical distribution—emergency power
- Navigation/ communications equipment
- Airport Emergency Command Post
- Electrical substations (local / regional)

Appendix C Figure B-8— ATC Tower

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 does not result in downstream consequences that create a more hazardous situation or impede operations.

1. Blast-Protection Protocols

a. Blast Envelope

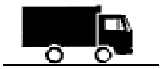
Typical security protocols involve the establishment of security perimeters, or rings, that act as filters to keep potential threats from their targets. In this case, during higher threat potential, vehicle restriction would be imposed by the TSA to keep LVIEDs from the terminal. This system of rings 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 and Explosives (BATF) have identified some basic vehicle sizes and explosive carrying capacities, as shown in *Appendix C Table C-1*.

By basing blast analyses on these carrying capacities, an airport can have a 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*).

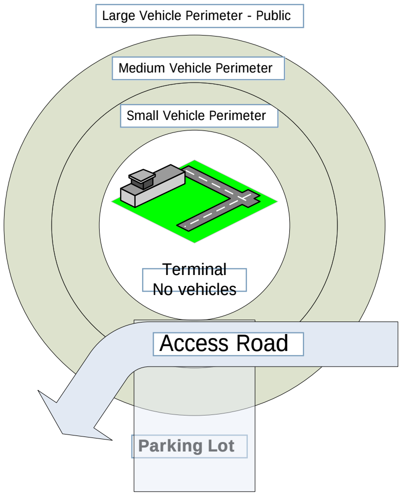
b. Vehicle Inspections

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.

ATF	VEHICLE DESCRIPTION	MAXIMUM EXPLOSIVES	LETHAL AIR BLAST	MINIMUM EVACUATION	FALLING GLASS
	COMPACT SEDAN	500 Pounds 227 Kilos	100 Feet 30 Meters	1,500 Feet 457 Meters	1,250 Feet 381 Meters
	FULL SIZE SEDAN	1,000 Pounds 455 Kilos	125 Feet 38 Meters	1,750 Feet 534 Meters	1,750 Feet 534 Meters
	PASSENGER VAN OR	4,000 Pounds 1,818 Kilos	200 Feet 61 Meters	2,750 Feet 838 Meters	2,750 Feet 838 Meters
	SMALL BOX VAN	10,000 Pounds 4,545 Kilos	300 Feet 91 Meters	3,750 Feet 1,143 Meters	3,750 Feet 1,143 Meters
	BOX VAN OR WATER/FUEL	30,000 Pounds 13,636 Kilos	450 Feet 137 Meters	6,5000 Feet 1,982 Meters	6,500 Feet 1,982 Meters
	SEMI-TRAILER	60,000 Pounds 27,273 Kilos	600 Feet 183 Meters	7,000 Feet 2,134 Meters	7,000 Feet 2,134 Meters

Appendix C Table C-1—Examples of Vehicle Explosives Capacity

Vehicle inspections should be conducted away from the airport's critical infrastructure, and in a location where vehicle congestion will have minimal effect on the local community. It is often good to have inspection points placed in a manner that allow vehicles to turn around or away from the inspection point, since some of the larger vehicles (e.g., construction trucks) may not be possible to inspect. It is important that these alternative routes do not lead to the terminal; they are not to be considered as bypass routes, but as routes to lead vehicles away from the inspection area, perhaps into a remote parking area instead. Care should be taken to ensure that any potential alternative route is securely blocked so that uninspected vehicles cannot gain access to the terminal or other critical infrastructure.



Appendix C Figure C-1

Blast Envelope

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 (not to clear out) possible explosive devices or vehicles. Once an IED is suspected, only the responding bomb squad can actually clear the device or determine its safety.

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.

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.

Limitations: When the design blast pressure is exceeded, large "panels" of the hardened windows tend to fail. A secondary "catcher" system behind the windows may also be needed. Window films offer no ballistic resistance. The aesthetics of the window hardening film should be considered. Some of the film systems require a thick bead of caulking at the window edges. Other systems require extensive window frame reinforcing. A mock-up of an in-situ window panel should be performed prior to implementing this material.

b. Conventional Window Replacement

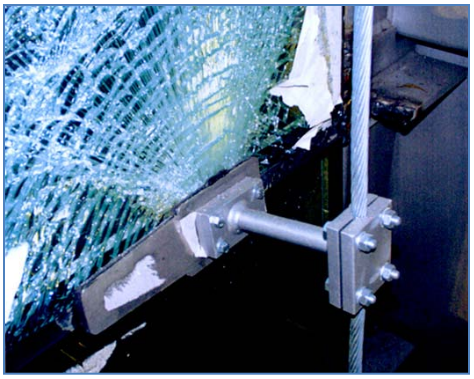
Current "state-of-the-art" window replacement systems can resist peak blast pressures of approximately 10 to 20 pounds per square inch (psi). Blast-resistant window systems should be laminated and/or thermally treated glass. A catcher system can be installed behind the windows to augment the performance of laminated glass systems. Replacement windows can also provide ballistic protection if required.

Limitations: Very few full-scale blast tests of replacement window systems have been performed. Most tests have been performed on small window panels in rigid window frames. This testing may not accurately reflect actual in-situ conditions for large curtain walls. Blast-resistant glazing requires special detailing and design.

c. High-Energy Absorbing Window Systems

Blast analysis and some testing have been performed on curtain wall systems that absorb blast energy rather than trying to reflect it. The analysis shows that very high blast pressures can be absorbed. By absorbing the blast energy, the effective pressure on the glazed panels is reduced significantly. Thus, the windows can be thinner and less costly. High-energy absorbing window systems can replace existing curtain walls or be installed behind existing glass and doorways to provide transparent blast protection.

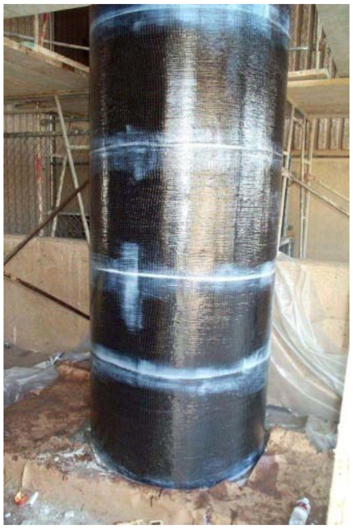
The fractured glazing image (refer to *Appendix C Figure C-4*) shows a successful blast test of a "high energy-absorbing cable-supported curtain wall glazing system."



Appendix C Figure C-2

High Energy-Absorbing Cable-Supported Curtain Wall Glazing System

d. Column Wrap



Kevlar and carbon fiber wraps (refer to *Appendix C Figure C-5*) can substantially improve the blast resistance of reinforced concrete columns. These systems have been installed in several retrofit conditions.

Limitation: The column wrap will affect the visual surface finish and texture of the columns.

Appendix C Figure C-3

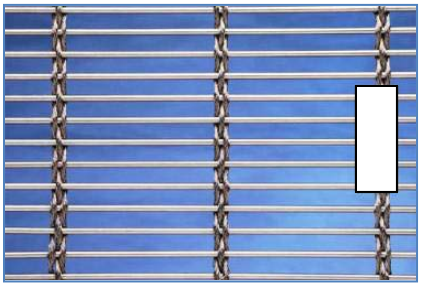
Column Wrapping Procedure

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 for medium-size IEDs.



Appendix C Figure C-4

View of Metal Fabric Catcher System

g. Polyurethane/Polyurea Elastomer Coating

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

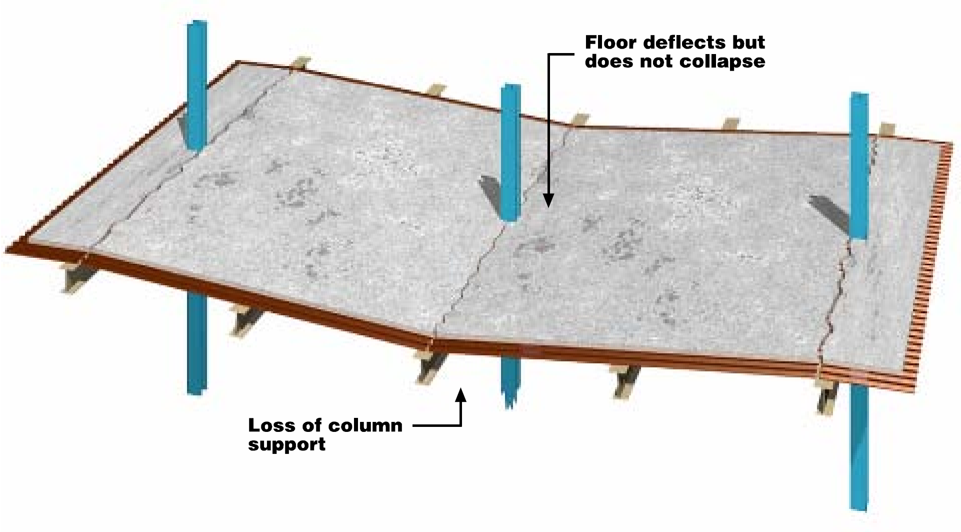
Testing and analysis has shown that a composite wall system (refer to *Appendix C Figure C-7*) can provide blast and ballistic protection from LVIED size bombs at close proximity.

Appendix C Figure C-5

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*).



Appendix C Figure C-6—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*) and elevated structures.

Limitations: Aesthetic and operational issues should be considered prior to deploying vehicle barriers. Operational issues resulting from narrowed roadways, including fire truck and emergency vehicle access, should be considered prior to erecting vehicle barriers.

Appendix C Figure C-7

Vehicle Barrier—At Grade

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* and *Appendix C Figure C-11*). 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*). Some models can contain chemical and biological gasses as well.

Appendix C Figure C-8

Large IED Threat Containment Vessel

Appendix C Figure C-9

Small IED Threat Containment Unit

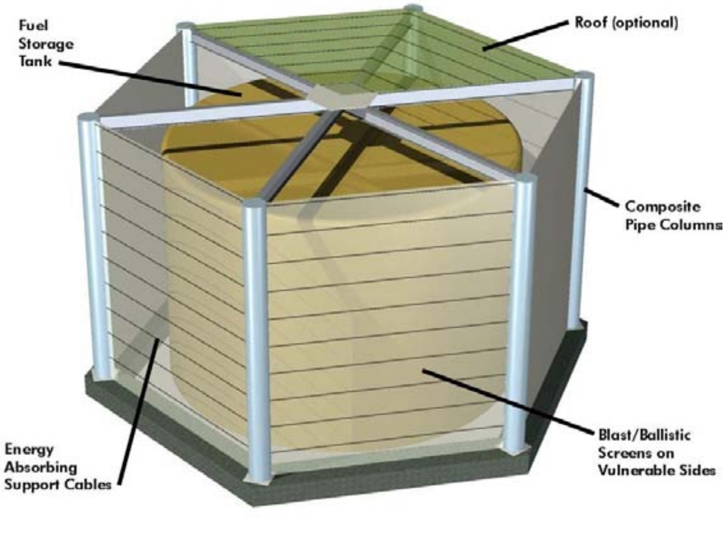
A mobile Threat Containment Unit (TCU) (refer to *Appendix C Figure C-11*) is capable of providing safe storage of small IEDs (7 pounds of TNT).

Limitation: The portable TCU cannot contain chemical and biological agents when dispersed with explosives.

m. Fuel Storage Tank Protective Screen

To protect fuel tanks, substations, and related equipment, a blast/ ballistic screen assembly (refer to *Appendix C Figure C-12*) can be installed to shield this equipment from most car bombs and high-powered rifle attacks. The screen material would likely be Kevlar or ornamental plate steel, depending on the threat. The screens are hung from energy absorbing steel cables that dampen the blast energy tremendously. The columns that support the screens likely would be constructed of steel pipes filled with concrete (composite columns), which have excellent blast-resistance and strength properties.

When constructing new fuel tanks for aircraft or rental cars at airports, consider buried tanks or recessing the tanks in a pit such that the tanks are



Appendix C Figure C-10

Blast and Ballistic Screen Assembly for Fuel Storage Tanks

not visible above grade and difficult to target with small arms. Also, when the tanks are recessed below grade, the surrounding soil helps mitigate the resulting blast if they are detonated.

n. Baggage Inspection Room

Baggage screening rooms offer little protection to the surrounding terminal facility, passengers, TSA baggage inspectors, or the police bomb squad contacted to assess and de-fuse a suspect IED. Current TSA protocol dictates that suspicious bags identified by in-line baggage screening devices are tagged for secondary "visual" inspection. Subsequently the suspect bag is re-directed to the bag inspection room for a visual inspection by opening the suspect bag and observing the contents. Opening the suspect bag might inadvertently detonate an IED or the bag itself may have a detonation trigger. If an IED is discovered, the TSA is directed to immediately leave the area, notify the bomb squad, and evacuate all or a portion of the airport terminal building.

Items to consider for improving the safety and operations of the baggage inspection room include the following:

1) Perform drills at all bag screening rooms to observe the action of the TSA and bomb squad if an IED is discovered while opening a bag. The "Threat Containment Unit" (TCU) access and response time would be evaluated and improved as needed. Also the communication protocol will be observed and clarified or modified if needed.

2) Consider placing an explosive disposal container capable of resisting a five to seven pound IED within or near the baggage screening room. A blast resistant trash container, for example, could be used for this. The bomb squad may elect to place the IED in this container prior to disarming or transporting the device out of the terminal building.

3) Consider hardening the bag inspection room. There are a variety of blast resistant, cost-effective wall, window, column, and ceiling system measures that can readily harden the room. For example, a wall and ceiling constructed of metal panels with the cavity filled with sand is very cost-effective and able to effectively mitigate small IED devices. A blast resistant skin can be added (retrofitted) to the existing walls to help mitigate an IED.

4) Evaluate and move critical services, utilities, and distribution systems away from the bag screening rooms.

5) Provide a wash station and shower in or near the bag screening room so that TSA personnel or the bomb squad can shower and wash off potential chemical and biological agents.

6) Provide a tightly sealed room and doors with a dedicated ventilation and filtration system so that chemical/biological agents can be contained.

7) If possible, move the bag screening rooms to locations that are accessible to the outside and can vent blast pressures outward.

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. This survey will assist in identifying areas and components of the airport that are vulnerable to acts of terrorism or sabotage, in particular, some areas that may have changed since the previous survey.

Section E—Blast Analysis Tools

Many blast analysis tools are available to evaluate and predict the effects of blasts on a building structure. It is important that the engineers using these tools understand the proper use and limitations of this software. Access to blast analysis programs is usually limited, and engineers must be authorized in order to obtain these security-sensitive programs.

The level of detail presented and used in a blast analysis can vary to extremes. Desired level of detail is a direct function of cost—extremely detailed analyses can be very expensive, while simpler and less expensive ones may be sufficient for the facilities being evaluated.

Engineers should evaluate the propensity of their structures to succumbing to progressive collapse. This is an important aspect of any good blast analysis. The removal of a key load-bearing structural member may propagate the failure of other key structural components throughout the facility. The consequences of such a failure are obvious. Such an attack achieves the desired result not by blast force and fragmentation, but by structural failure. Many of the blast analysis software programs available do not take into consideration the transfer of the dead loads of the missing structural member to other surrounding members and their subsequent ability to support those additional loads. This type of evaluation is usually performed separately from the blast pressure load calculations.

Guidance for conducting blast analyses can be found in the Federal Emergency Management Agency's Manual 426, "Risk Management Series: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings." Chapter 4 of this document discusses different methods by which designers can assess potential damage to their facilities.

APPENDIX D
GENERAL AVIATION

Recommendations here are generally tailored for general aviation (GA) operating areas located at airports with commercial [scheduled passenger airline] service and regulated under Transportation Security Regulation Part 1542. Commercial service airports, as well as airports serving only general aviation aircraft, can find additional information specific to GA in TSA's Security Guidelines for General Aviation Airports. Operational recommendations, such as establishing a community watch program and the use of auxiliary aircraft locking devices, may also be found there.

1. Introduction

General aviation (GA) refers to all aviation except commercial scheduled passenger airlines and the military. The approximately 200,000 general aviation aircraft constitute about 75 percent of all U.S. air traffic. General aviation operations are typically asymmetric and passengers of GA aircraft do not undergo screening, except under certain limited conditions. Passengers aboard the GA aircraft are typically known by the pilot in command, who has final authority over what items may be carried on board a GA aircraft.

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

2. Security Areas and Boundaries

As discussed in Part III, Section B, Airside, it is advisable to exclude general aviation operating areas from the SIDA of the airport as much as is practicable. In the event this is not possible, operational limits should be considered to eliminate any possible breach of Part 1542 security. GA passengers, crews, cargo and baggage should be screened when entering sterile areas; or alternatively, GA passengers, crews, cargo and baggage should proceed through clearly marked areas away from sterile areas.

a. At commercial service airports where the Aircraft Operating Area (AOA) precludes separate fencing or barriers for the GA aircraft operating area, clearly marked signage and ground markings are important to prevent GA operators from inadvertently crossing into SIDA or sterile areas of the tarmac.

b. When addressing security controls of GA operations and persons at commercial airports, the principle to be followed is that of complete separation from commercial traffic.

c. Separation is normally accomplished by designing general aviation parking areas that lie outside of areas secured for commercial operations.

d. Design ramp parking arrangements to ensure visual observation of aircraft and passengers during the embarkation and disembarkation process.

3. Ramp Security Measures

FBO/GA terminal operators should consider the design of secure or monitored access doors and gates for each portal leading to the aircraft ramp. Provide signage that clearly restricts access to the aircraft operations area to authorized persons only.

4. Signage

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

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

AOPA's
AIRPORT
WATCH
REPORT SUSPICIOUS ACTIVITY
1-866-GA-SECURE
(1-866-427-3287)
FOR EMERGENCIES
911

Appendix D Figure D-1

AOPA Airport Watch Sign

5. **Lighting and Cameras**

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

- Aircraft parking and hangar areas;
- Fuel storage areas and fuel trucks;
- Airport access control points; and
- Other appropriate areas, such as vehicle parking, fences or obstructed areas.

6. **Based Aircraft**

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

7. **Building Design Factors**

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

a. The Customer Service Representative (CSR) Reception area should have a clear view of all doorways and other access points leading to the ramp.

b. Hangar access should be controlled and restricted to authorized personnel only. In some circumstances, the GA area access controls may be tied to the airport access control and alarm monitoring system.

c. Ramp access from the FBO or Terminal should be controlled and restricted to authorized personnel only.

d. Vehicle access, including pilot, passenger, taxi, livery or delivery access to the ramp should be monitored via CCTV or visual inspection to establish a positive identification prior to operating the gate access control to the ramp. Separate the driver from the vehicle if necessary to ensure the driver is not under duress.

e. Consider minimizing ramp access by all vehicles as much as possible.

8. **International General Aviation**

Where possible, the design of separate CBP or Federal Inspection Areas should be incorporated using the design standards for a general aviation FIS facility. Review Chapter 8, “General Aviation Facilities,” of the Customs and Border Protection document, Airport Technical Design Standards.

APPENDIX E

PLANNING & DESIGN SUPPORT OF COMMAND AND CONTROL

Section A—Introduction

Airport Command and Control (C2) centers are extremely challenging environments to design and build. Digital platforms will support multiple operational functions, including security, and add Information Technology (IT) to the C2 center design. This outline will assist airports in planning and designing their C2 facilities, which are not required by regulation.

Section B—Operational Considerations in Project Planning

1. Concept of Operations

As the number and complexity of systems increases, it is important to recognize the need for a Concept of Operations (ConOps). The term ConOps refers to the need to consider and document how an airport's operations will be conducted, including operational response to events to ensure that all elements and assets of an organization are synchronized to respond.

The Critical Infrastructure Key Resource (CIKR) Annex from the U.S. Department of Homeland Security National Response Framework (NRF) provides the following definition of ConOps:

> *The concept of operations describes specific organizational approaches, processes, coordinating structures and incident-related actions required for the protection and restoration of CIKR assets, systems, networks, or functions within the impacted area and outside the impacted area at the local, regional, and national levels.*

The airport ConOps planning should be used as a driver for the development of security technologies and facilities. Airport ConOps plans should be reviewed by security design professionals to harmonize with the planning and design of technology and facilities. Where security design cannot be adapted to ConOps requirements, there should be recognition of that fact and adjustments made to address the design constraints.

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

a. Airport Security Program: The ASP is developed pursuant to 49 CFR Part 1542, which governs the overall security arrangements for the airport. It addresses matters such as perimeter security, access control, surveillance, contingency plans, and law enforcement response.

b. Emergency Operations Plans: An Airport Emergency Plan (AEP) for a variety of incident responses is mandated under 14 CFR Part 139 and is coordinated with the ASP requirements. It's often aligned with State or local emergency operations plans where the airport may have defined responsibilities, e.g., designation of an airport as a strategic logistics supply point in the event of an emergency; or as a strategic national stockpile distribution reception point in the event of a pandemic).

c. Incident Action Plans: A plan reflecting the overall strategy for managing certain incidents, and not necessarily requiring formal long-term planning. It may include the identification of operational resources and assignments, as well as provide management with information on the incident.

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

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

2. Transition

Whether building new or upgrading a Command and Control facility, plan for the logistics of staging equipment and the transition phase between old and new facilities.

Create a Transition Plan that details the transition of each system, component, and staff from the old to the new facility. Each element should have a contingency plan that details what will happen if a system becomes inoperable or unavailable. Before new computer-based systems are implemented in the Command and Control facility, they should be tested in a staging facility.

Section C—Types of C2 Structures

The C2 function can use a variety of organizational structures to support a given ConOps. Some C2 structures operate 24 hours a day, 365 days a year; some handle a narrow range of functions, while some are oriented solely toward responding to emergencies of varying scale. The list below provides a primer on C2 structures commonly employed in the airport security arena:

1. Security Operations Center (SOC)

A SOC is the focal point for airport security monitoring, command and control (C2) and communications functions. These functions often involve sensitive security information whose dissemination needs special control. Generally, a SOC will be a 24/7/365 operation, staffed and designed pursuant to the guidance of the security ConOps and the ASP.

The SOC generally performs two principal functions:

a. It serves as a platform to collect information from a range of sources to provide situational awareness for command personnel. It serves as a platform for the exercise of command and control over the allocation and deployment of security resources and capabilities. A SOC can be designed to leverage multiple communication links throughout the airport, including police, fire/rescue, airport operations, off-airport emergency assistance, and secure communication channels to Federal, State, and local agencies. These communication links may be used for the allocation of resources, the gathering of information, and/or for coordination of action.

b. The SOC should include coordination of security functions with other command and control functions, including physical or virtual linkage with other operations, e.g., Airport Operations Center (AOC), Emergency Operations Center (EOC) and Incident Command Post(s) (ICP). (See RTCA DO-230C, Integrated Security System Standard for Airport Access Control.)

2. Airport Operations Center (AOC)

An AOC is the focal point for daily airport operational functions including, but not limited to, issues such as maintenance of the airfield, runway surface, and lighting; and the management of terminal facilities and fueling facilities. It might also include control over gate operations and aircraft maintenance areas (though these may be tenant functions). Generally, this will be a 24/7/365 operation; its design should support the ConOps for airport operations, including linkage the SOC and EOC in the event of an incident, because many security events will profoundly affect the continuing daily operations of the airport.

3. Public Safety Answering Points (PSAP)

An airport PSAP can serve as the focal point for 9-1-1 service to a larger geographic area outside its fence, receiving and processing emergency calls and event notifications for a specific area. These facilities dispatch public safety personnel such as police, fire, and EMS in response to calls for service. PSAPs should have the flexibility to include additional operators during emergency situations.

4. Fusion Center

Multiple agencies can collaborate to provide resources, expertise, and information to the center with the goal of maximizing the ability to detect, prevent, investigate, and respond to criminal and emergency activity. The airport is usually a participant / user rather than the host agency. Ideally, the fusion center involves every level and discipline of government and private sector entities, although the level of involvement will vary based on specific local circumstances.

5. Emergency Operations Center (EOC)

   The physical location at which information and resources support incident management and on-scene operational activities. An EOC may be a temporary facility, or may be located in a more permanently established facility, often near the SOC/AOC. It may be organized by major functional disciplines (e.g., fire, law enforcement, medical services), by jurisdiction (e.g., Federal, State, regional, city, county), or by some combination thereof.

6. Incident Command Post (ICP)

   The field location where the primary functions are performed. The ICP may be co-located with other incident facilities.

There are myriad physical configurations that can be designed and constructed to accommodate these C2 structures. The guidelines offer a comparative perspective concerning the design requirements; it is understood that choices may be constrained by resource limitations.

Section D—Three Tenets of C2 Facility Design

The three main tenets of design that should be followed in C2 Center design are:

1. Reliable

   The C2 facility should be reliable in order to achieve its mission. This means that systems should be designed to perform under stress; be resistant to attack, both physical and cyber; and be rigorously maintained.

2. Flexible

   The C2 facility should be flexible enough to accommodate the unplanned conditions that arise during emergencies. Systems and spaces should be capable of adapting to new users, unforeseen circumstances, and extremely high intensity use.

3. Scalable

   C2 facilities are not static environments. As new technologies are introduced, the C2 facility should be capable of growing and supporting these new technologies, to avoid obsolescence.

Section E—Design Process

1. Choosing the Design Team

   a. Choose an architect/engineer with experience in C2 facilities. There are many operational nuances unique to C2 facility design beyond the range of normal experience of most traditional architects and engineers.

   b. The technology designer is a key design team member. A C2 facility is not merely an architectural and engineering effort; the technology is interwoven into the operational systems; a technology designer should be involved from the project's inception.

2. Site Selection

   a. Geographic location is extremely important. Assess your geographical threat profile using FEMA and other data to determine threats, e.g., flooding, storms, etc. Don't locate a C2 facility next to areas that are inherently risky.

   b. Plan for appropriate non-standard access during emergencies. Consider the difficulty of gaining access to AOCs inside the airport when the perimeter becomes locked down. During emergencies, this includes access for first responders, outside staff, and parking and logistical spaces.

c. Plan for logistical support. During emergencies, it's common for staff to occupy the Command and Control Facility for long periods of time. This may require food and supplies and added computer or communications equipment. Ensure there is adequate power, IT bandwidth, space and access for deliveries and people, and possibly sleeping and bathing facilities

d. Locating the C2 facility within the building can have a significant impact on survivability, cost, and usability:

1) If possible, locate it where it has the most physical protection from threats. Locating in a basement or ground floor may be subject to flooding; the highest floor of a building could be affected by storms or high winds). Avoid exterior walls and windows because of projectiles or explosions. If an exterior wall or window cannot be avoided, use wall reinforcing techniques or window blast curtains.

2) A C2 facility will require a data center with large-capacity utilities like power and cooling. While the data center need not be immediately adjacent to the C2 facility, a greater distance creates greater costs for network and cabling connectivity and possibility of disruption.

3. Space Design

Different Profiles for Different Missions: Command Centers can have many different profiles, each with a unique focus on a specific mission.

- Emergency Operations Center (EOC) is focused on managing emergencies. An EOC is often not occupied until it is "activated" when an incident occurs. Technology infrastructure should be designed to accommodate unfamiliar outside users from multiple organizations and should be scalable for the sudden influx of people when emergencies occur.
- Airport Operation Center (AOC) focuses mainly on the day-to-day operations of a complex facility, such as an airport. The AOC manages routine work that is essentially the same every day, with occasional emergency response activities. AOCs may include monitoring building functions such as building automation and asset and maintenance management.
- Security Operations Center (SOC) is the facility that manages video surveillance, alarms, access control, and other day-to-day security systems. SOCs support both routine work as well as frequent coordination with emergency response activities. SOCs frequently employ large-format video displays for displaying multiple video surveillance feeds.
- Public Safety Answering Points (PSAPs), also known as 9-1-1 centers, are charged with managing public safety personnel, such as police, fire, and EMS.
- Fusion Centers are designed for the interaction of multiple organizations in a facility that encourages collaboration. Fusion Centers are typically utilized by government agencies to collaborate on intelligence issues, and exchanging knowledge not easily communicated via more formal channels of communication.

a. Consider Co-Locating Multiple C2 Facilities to Leverage Infrastructure and Reduce Overall Cost

It is sometimes desirable to co-locate two different types of Command Centers in the same facility. For example, having an EOC next to an AOC/SOC can have definite advantages during emergencies, allowing easier communications among emergency managers other groups. However, poor design can have a negative effect if the commotion of the EOC is allowed to impact the AOC/SOC environment. Architectural approaches such as glass walls/doors or moveable walls provide the flexibility to achieve collaboration without disruption. Glass walls or doors can also allow visual communications between EOC and AOC/SOC staff, as well as enable sharing of visual resources like video walls.

b. Ergonomics

1) Design with staff comfort in mind to reduce stress and improve performance:

a) Be careful of lighting design to prevent glare. C2 facilities are not typical office environments, where lighting is often too bright. A C2 facility operator is visually focused on computer screens and large format video displays.

b) Design for sound management. During emergencies, C2 facilities can become very noisy due to the number of people and the level of activity. Use techniques such as electronic sound masking and sound deadening materials to avoid aural overload.

2) Sightlines: Provide the necessary visual resources, such as video walls and other large-format visual displays. Ensure that managers have unobstructed sightlines to communicate with staff (many times, a gesture or facial expression can be a means of communication in an emergency). At a minimum, do sightline studies and conventional renderings and, if possible, utilize 3D digital models.

3) Traffic Patterns: Ensure that staff can move around within the space without causing disruption. Place resources like copier machines in areas where staff can easily access them without encroaching on others' work spaces.

4) Seating: Ergonomic seating can increase attention spans and reduce repetitive strain injuries.

5) Consider Alternate Desk and Console Designs: Newer desks and consoles are designed to reduce fatigue and stress, e.g., consoles that are movable up and down allow staff to sit or stand.

6) Computer Monitors: Choose monitors with appropriate resolution, dot pitch, brightness, and contrast to reduce eye strain and increase comprehension.

c. Design for Flexibility During Emergencies

The profile of the C2 facility changes during emergencies because Command and Control Facilities tend to fill up when emergencies occur. Flexible design elements like moving walls, and sliding glass doors, etc., allow easy reconfiguration as needed.

d. Media Access

Ensure the press area is segregated from the rest of the facility to prevent security breaches.

e. Meeting/break out rooms

Include spaces for private meetings, possibly located adjacent to the C2 facility with glass walls or windows that allow private conversations while maintaining visual contact with the main activities.

f. Staff Support Spaces

Plan break rooms in proximity to the C2 facility to accommodate staff. Providing break rooms and/or a kitchen will encourage staff to stay on-site rather than leaving the facility for lunch or breaks. Sleeping rooms can be useful during long-term emergencies.

g. 3D Design Simulations

Utilize advanced design techniques like 3D simulation when possible. C2facilities are complex environments that can be difficult to visualize. Using 3D modeling allows you to "walk through" the design and accurately visualize sightlines and other nuances not visible in a 2D construction drawing.

4. Infrastructure Engineering

The infrastructure of a C2facility, while sharing many similarities with commercial buildings, diverges significantly in the design process that determines adequate capacities and other attributes.

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

b. Heating, Ventilation, and Air Conditioning (HVAC) will be one of the key needs for the Command and Control Facility due to the amount of electronic components contained within. Remember that HVAC is one of the costliest elements to retrofit after construction is completed, so better to slightly over-design (and accommodate future expansion) than under-design.

c. Structural attributes like blast and high wind resistance should be considered when designing new structures. When retrofitting existing structures, blast netting and other retrofits should be used.

d. Network/Internet access should come from multiple sources to provide redundancy. Check with Internet Service Providers to secure connections from multiple sources, including possible satellite connectivity as a backup.

e. Envelope electromagnetic/lightning protection should be part of the design, and shielding from electromagnetic pulse (EMP) may be warranted in certain Command and Control Facilities.

f. An alternate potable water source could be invaluable in long-term emergencies when local utilities are not available.

g. Wireless signal penetration is often an issue. Depending on the location, it may be desirable to either enhance penetration of wireless signals from outside, or to block them. Wireless signals from cell phones, public safety radios systems, GPS, satellite, and other wireless communications should all be considered.

1) To block wireless signals to prevent unauthorized communications, the use of a “Faraday Cage” technique is effective. By enclosing an area in a wire mesh, it is possible to block wireless signals. Wall coverings, ceiling tiles, and other building materials with inherent wireless shielding are available.

2) To enhance wireless reception inside the facility, wireless repeaters may be necessary when the building’s structure blocks signals. Design for multi-band repeaters that will work with all the wireless devices use should be considered.

h. Resupply and storage space for essential supplies, such as food, fuel for a generator, batteries, and office supplies, etc., should be considered in the design.

i. Satellite dishes will require space on the roof and line-of-sight access to satellites. They will also need periodic maintenance. Plan roof layouts and access accordingly.

j. Elevators should be large enough to handle Data Center equipment, which may include moving entire racks of equipment weighing as much as 1,000 lbs or more. Elevators should have power backup.

5. Systems/Components in the C2 Environment

a. Consoles and Furniture

Older C2 systems were component-based, directly operated by the users using knobs and switches. This direct human-machine manual interface required consoles to enclose, protect, and aesthetically hide equipment. Modern facilities exclusively utilize computer-based systems housed in a Data Center, with human-machine interaction, connected remotely to the operators’ desktops through a network using KVM (Keyboard/Video/Mouse) extension technology. Computers last longer and are easier to secure and service in a Data Center.

In this environment, true consoles may not be a necessity, and it may be possible to use lighter, less costly, re-configurable furniture that allows more flexibility. Users can quickly move positions by relocating their keyboard, mouse, and screen to a different network connection.

b. Large-Format Video Displays Now Impact Command Center Design

Carefully consider the design of large-format visual displays. Designing for large-format displays requires a cross-disciplinary approach that includes an understanding of technology and ergonomics as well as traditional architectural/engineering concepts. Refer to the chapters on CCTV/Surveillance and IT/Communications. Some critical design aspects include:

1) ConOps (Concept of Operations): It is critical to understand how the displays support ConOps, including what will be displayed, who will view it, and who controls it.

2) Display Placement: Determining where a large-format video display is located is not as simple as finding empty wall space. It is crucial to understand sight lines to manage such issues as light refraction, light levels, and acoustic attributes such as sound transmission and ambient noise management. Placing a display in the wrong location could result in glare and reflection from windows, inhibiting the ability for staff to see details on the screen.

3) Support infrastructure: Each large-format display requires power, cooling, and cabling—elements that should be addressed in the design phase. Large-format displays are not just big television sets; they are complex computers and require a similar, high-tech design approach.

4) Integration with other systems: Video displays are no longer confined to displaying surveillance camera feeds or television broadcasts. Today's video displays are a window into the full spectrum of systems and information sources from anywhere inside or outside the airport. Current control systems for video displays can connect to and display a huge range of visual information, including video surveillance cameras, computer screen content, documents, software applications, television, and video conferencing.

c. Redundancy in IT Systems

Critical applications and components should have redundant backups that allow for component failure without compromising systems' operation.

1) Server clusters provide for failover to backup servers in milliseconds, with no noticeable delay for users.

2) RAID (redundant array of independent disks) provides increased storage reliability and protection against data loss through redundancy.

3) Network switches and routers should utilize redundant components.

4) Data backups should be performed periodically, and off-site backups should be considered as a safeguard against complete facility compromise.

6. Cyber Security

Because of the computer-based architecture of today's security systems and the interconnected nature of the Web-based world, it is imperative that all systems are secured against cyber threats. This topic is far too complex to cover in this document, but Command and Control Facility designers must create a plan for cyber security that addresses design challenges like firewalls, virus detection, intrusion detection, and identity management.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F

INTERNATIONAL AVIATION SECURITY AND IMPLICATIONS FOR U.S. AIRPORTS

1. U.S. Customs and Border Protection Facility Requirements

Federal Inspection Services (FIS) facilities are required at all U.S. airports which process passengers arriving on international flights. FIS facilities consist of passenger processing areas including support spaces for offices, maintenance, telecommunications, and other functions and are designed in accordance with law enforcement requirements, unique FIS security considerations, and disaster / management crisis criteria. The FIS area is defined in terms of passenger / baggage flow, inspection process criteria, terminal building space utilization and supporting administrative and operational space.

When international terminal planning begins, security design and construction requirements will be determined for the FIS area by U.S. Customs and Border Protection (CBP) and several other Federal agencies utilizing FIS to clear arriving international passengers. FIS areas are also required at pre-clearance stations located outside of the United States, where the designated FIS area is a restricted area reaching from the primary processing area to the departing aircraft, including all areas in between. FIS space requirements will vary according to the CBP standards for small, medium and large airports; these differences should be coordinated at the beginning of the design process with CBP as lead Federal stakeholder.

While Federal inspection services are furnished by the government at no cost to the airport, airport operators are required by law, at their 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.

The CBP Airport Technical Design Standards (ATDS) reflect national policy, procedures and facility development standards for the design and construction of CBP facilities at U.S. airports and foreign preclearance facilities. Other Federal agencies will also be present within the FIS facility, including but not limited to the Public Health Service (PHS), U.S. Fish and Wildlife Service (FWS), and U.S. Department of Agriculture (DOA).

a. CBP Mission Requirements

In accordance with CBP’s mission to secure the nation’s borders while facilitating trade and travel, FIS agencies process and control U.S.-inbound traffic to ensure persons, baggage and cargo are not concealing illegal substances or contraband. Likewise, FIS agencies monitor outbound international traffic to prevent transport across U.S. borders of illegal monetary instruments / controlled articles.

In support of its mission, CBP has established unified primary inspection processes at all United States ports of entry along with specialized secondary inspections focused on combating terrorism. CBP utilizes a number of technologies and processes to facilitate passenger processing, and will provide the airport operator with information on technologies as they impact design and construction processes.

b. FIS Space Requirements

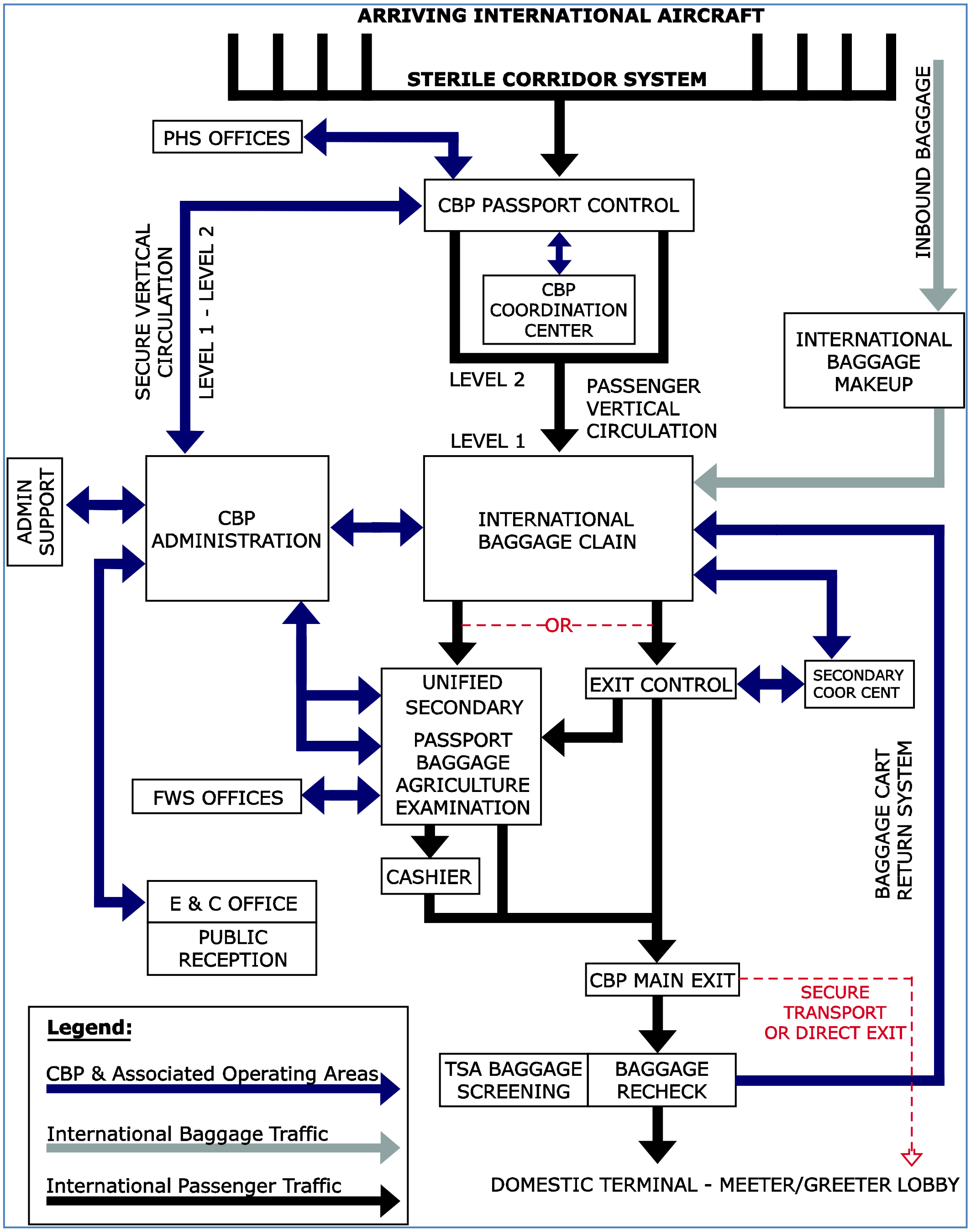
Airport facilities are classified by the maximum number of passengers processed at the peak hour of operation. Operational space requirements should be coordinated by the airport operator with CBP to determine specific requirements for each proposed facility in accordance with the ATDS.

Any changes to specified space requirements are handled by a change request process managed through CBP. Otherwise, space requirements should comply with the detailed space matrix embedded in the ATDS.

c. CBP FIS Flow Process

General FIS operations and functions are usually amended to reflect the unique requirements and flow process of the individual airport. Depending on facility configuration, there may be alternate flows for passengers connecting to international or domestic flights.

Initiatives such as the Trusted Traveler program and the Advanced Passenger Information Service will impact the processing of passengers through FIS; the ATDS contains information on coordinating these


ARRIVING INTERNATIONAL AIRCRAFT
STERILE CORRIDOR SYSTEM
PHS OFFICES
CBP PASSPORT CONTROL
CBP COORDINATION CENTER
SECURE VERTICAL CIRCULATION
LEVEL 1 - LEVEL 2
INBOUND BAGGAGE
INTERNATIONAL BAGGAGE MAKEUP
LEVEL 2
PASSENGER VERTICAL CIRCULATION
LEVEL 1
ADMIN SUPPORT
CBP ADMINISTRATION
INTERNATIONAL BAGGAGE CLAIN
OR
UNIFIED SECONDARY
PASSPORT BAGGAGE AGRICULTURE EXAMINATION
EXIT CONTROL
SECONDARY COOR CENT
FWS OFFICES
CASHIER
BAGGAGE CART RETURN SYSTEM
E & C OFFICE
PUBLIC RECEPTION
CBP MAIN EXIT
SECURE TRANSPORT OR DIRECT EXIT
Legend:
CBP & Associated Operating Areas
International Baggage Traffic
International Passenger Traffic
TSA BAGGAGE SCREENING
BAGGAGE RECHECK
DOMESTIC TERMINAL - MEETER/GREETER LOBBY

Appendix F Figure F-1

Example of Typical Flow Process for Arriving International Air Passengers

processes within FIS facilities. As these technologies develop, coordination with CBP will be critical to plan for their impacts on passenger processing flow.

Once an FIS project has been identified, the CBP Port Director and Field Office representative will meet with designers to refine the project requirements. CBP's Facilities Management and Engineering Directorate (FM&E) then appoints a project manager to coordinate with the Office of Field Operations (OFO), which is the office that determines the operational requirements for international airport facilities for CBP and performs CBP operations in the CBP area of the FIS. CBP FM&E office is the approving authority for project design and construction plans.

Consult the ATDS to determine the spaces and design considerations applicable to each type of airport facility. OFO will determine the calculated passenger throughput necessary to classify airport facilities.

The following flow diagram is typical of many FIS facilities, and is subject to a range of local and CBP constraints and adjustments to be negotiated with CBP. It is intended only to illustrate the complexity not only of the individual elements of the facility requirements, but the need for control of flow among them.

A preliminary rule of thumb suggests at least 80 square feet per peak hour international deplaning passenger (assuming an aircraft load factor of 90 percent) should be initially planned. A 215-seat aircraft, for example, would require space to service 194 peak-hour international passengers, or 15,500 square feet of FIS space, so early terminal design consultations with CBP to determine specific space and operational requirements are vital. Secure passageways to route deplaning passengers to the FIS area from the gates should be secured with CCTV cameras and access controls. Once completed and accepted for occupancy, all areas within the secure perimeter fall under the sole control of CBP who subsequently authorizes any physical access by airport / air carrier or other personnel as well as controls any future alterations to the facility.

d. CBP Airport Design Review and Construction Management Process

CBP reviews an airport's request for an FIS facility construction project to determine FIS operational / technical requirements and provides approval for those requests. The design process includes multiple levels of CBP stakeholder review until a complete set of construction documents is ready for bid. CBP coordination with affected agencies and stakeholders is required early and often throughout the design process to ensure that all associated requirements are met.

CBP has documented a detailed design review process in the ATDS that includes the responsibilities of all parties involved (Port, Field Office, OFO HQ, FM&E PM, A/E Contractor, and the airport.) and the authorities for each step of the process.

The process includes:

1) Request process, in which the airport provides CBP with a request for an FIS construction project to support a projected number /frequency of flights, from anticipated originating countries, and projected passenger loads. CBP reviews the request and provides approval and requirements to the airport.

2) In the pre-design and programming process, CBP reviews any approvals regarding space programming, site selection, concept development, functional adjacency, blocking/stacking diagrams, and long-term master plan.

3) Schematic design begins by detailing coordinates for room layouts, specifications, technical narratives (engineering systems), floor plans, and elevations for required CBP review and approval.

4) In the design/development phase CBP provides review and approvals for floor plans, finish schedules, engineering diagrams, security systems, and such special construction requirements such as detention rooms.

5) The construction phase begins coordination of construction documents, door schedules and access controls, etc., and moves into bid award, construction schedule and milestones for required CBP review and approval.

6) Upon completion of construction, CBP coordinates occupancy procedures, ensuring that furniture, computer, and equipment installations, resolution of punch-list, and commissioning for first flight arrivals are acceptable.

e. Airport FIS Planning and Design Issues

The ATDS provides information on applicable codes, regulations, equipment specifications, technical standards, security requirements, data and telecommunications requirements, signage, and other parameters. Requirements related to physical security and information technology are constantly changing, as outlined elsewhere in this Guidelines Standard, and should be coordinated with CBP.

System Integration and Networking: The advent of new technologies, including data networks capable of transmitting live video images and voice telephony integration with airport systems may result in improved cost-effective design at some airports. Airport security monitors activity throughout the airport property while CBP employs agency-dedicated surveillance cameras to monitor U.S.-inbound international passengers, air crew members, baggage, and cargo. At pre-clearance sites outside the U.S. CBP cameras can monitor the processing area, passenger/baggage holdrooms, and U.S.-bound aircraft parking ramps.

2. Flights Arriving from Pre-clearance Facilities

U.S. CBP has expanded its pre-clearance stations with the addition of new facilities and the conversion of legacy facilities to full pre-clearance facilities. In addition to typical CBP clearance processes, local screening authorities undertake security screening for checked bags and passengers. Pre-cleared passengers deplane into U.S. domestic terminals, mix with other domestic passengers, and are free to leave the terminal building or to undergo pre-board screening if boarding connecting flights.

Rules clarified in 2003 stipulate that connecting bags from pre-cleared flights must be re-screened through certified equipment before the next enplanement. The method to meet this requirement varies from airport to airport depending on the distance from checked baggage screening facilities and the method of routing bags to that location.

3. Impacts on U.S. Airports of Foreign Security Requirements and Initiatives

ICAO Member States enplaning last-point-of-departure flights into the United States must meet a host of CBP, ICAO and TSA security requirements. Growing use of enhanced screening technologies and threat-based or random screening for passengers on U.S.-bound international flights are also key areas of change.

Greater risk assessment information processing using advanced technologies (electronic Advanced Passenger Information Systems (eAPIS), Passenger Name Record (PNR) data, etc.) as well as cooperative initiatives among aviation and FIS stakeholders continue to evolve and impact U.S. international arrivals processes and should be carefully monitored by airport operators.

Part IV-Appendix F—International Aviation Security Checklist:

□ **Model the proposed design to ensure clear and unambiguous passenger flow.**

□ **Model various processing times and passenger flows through exit control.**

□ **Life safety issues vs. security requirements have equal footing.**

□ **Establish a task force to review design parameters, document changes, and agreements.**

□ **Changes will occur; establish protocols for review of changes.**

□ **Coordinate w/ FIS Security Plan**

- Contact CBP; Federal Agencies
  - Obtain CBP Airport Technical Design Standards
  - Obtain Workforce Analysis Model (WAM).
- Address Issues in FIS Plan
  - Physical Safeguards
  - Plans/Procedures for Implementation
  - Resources to Sustain FIS Protection Program
- Coordinate FIS Security Plans and Requirements with ASP
  - Access Control
  - CCTV
  - Baggage Screening and EDS
  - Perimeter Protection

- ▸ Video, Voice, and Data Networking

□ **FIS Design, Construction, Acceptance and Occupancy**

- ▪ Provide for CBP/Agency Involvement in Specifications, Drawings, and Construction Documents
- ▪ Schematic Design
  - ▸ Model variability in processing times using the CBP Model
    - Architectural Integration
    - Security Integration
    - IT Integration
  - ▸ Construction Bid Package
  - ▸ CBP written approval at each step
  - ▸ Establish change review process

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G
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. Some definitions may not appear in this document, but are included to provide some clarity to complex issues that continue to evolve from previous versions of the document.*

A/C Advisory Circular (FAA)

ACAMS Access Control and Alarm Monitoring System

Access Control A system, method or procedure to limit and control access to areas of the airport. 49 CFR 1542 requires certain airports to provide for such a system.

ADA Americans with Disabilities Act

AEP Airport Emergency Plan

AIP Airport Improvement Program (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).

Air Carrier An entity or person who undertakes directly by lease, or other arrangement, to engage in air transportation. Also known as Aircraft Operator. This includes an individual, firm, partnership, corporation, company, association, joint-stock association, governmental entity, trustee, or similar representative of such entities.

Air Carrier Aircraft An aircraft that is being operated by an air carrier and is categorized, as determined by the aircraft type certificate, as either a large air carrier aircraft if designed for at least 31 passenger seats or small air carrier aircraft if designed for more than 9 passenger seats but less than 31 passenger seats.

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 A person who uses, causes to be used, or authorizes to be used an aircraft, with or without the right of legal control (as owner, lessee, or otherwise), for the purpose of air navigation including the piloting of aircraft, or on any part of the surface of an airport.

Aircraft Stand A designated area on an airport ramp intended to be used for parking an aircraft.

Airline An air transportation system including its equipment, routes, operating personnel, and management.

Air Operations Area
(also AOA)
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
An area of land or other hard surface, excluding water, that is used or intended to be used for the landing and takeoff of aircraft, including any buildings and facilities.

Airport Operating Certificate
A certificate, issued under FAR Part 139, for operation of a Class I, II, III, or IV airport.

Airport Operator
A person that operates an airport serving an aircraft operator or a foreign air carrier required to have a security program under 49 CFR 1544 or 49 CFR 1546.

Airport Ramp
Any outdoor area, including aprons and hardstands, on which aircraft may be positioned, stored, serviced, or maintained.

Airport Security Committee
A TSA-encouraged airport security committee made up of persons and organizations having a direct interest in the security decisions being made and their impact on the airport security environment. Participants might include airlines, concessions, other tenants, FBOs, and TSA representatives, among others. An Airport Security Committee is an advisory panel and a broad-based resource for airport security matters; it is not empowered to issue directives.

Airport Security Program
An airport-specific security program approved by TSA under 49 CFR 1542.101.

Airport Tenant
Any person, other than an aircraft operator or foreign air carrier with a security program under 49 CFR 1544 or 49 CFR 1546 that has an agreement with the airport operator to conduct business on airport property.

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

Alarm Resolution
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.

Approved
Unless used with reference to another person, means approved by TSA.

Apron
A defined area, on a land aerodrome, intended to accommodate aircraft for purposes of loading or unloading passengers, mail or cargo, fueling, parking or maintenance. Often called a ramp.

ARFF
Aircraft Rescue and Fire Fighting—A term used to identify the facility, operation or personnel engaged such activities.

ASC	Airport Security Coordinator—An individual designated by an airport operator to serve as the primary contact with TSA for security-related activities and communications.
ASP	Airport Security Program under 49 CFR 1542.101.
ASTM	American Society for Testing and Materials
ATC	Air Traffic Control
ATCT	Airport Traffic Control Tower
ATO	Airport Ticket Office—A place at which the aircraft operator sells tickets, accepts checked baggage, and through the application of manual or automated criteria, identifies persons who may require additional security scrutiny. Such facilities may be located in an airport terminal or other location, e.g., curbside at the airport.
ATSA	Aviation and Transportation Security Act of 2001
ATSP	Airport Tenant Security Program
AVSEC	Aviation Security
AVSEC Measures	Aviation Security Contingency Measures (contained in the ASP)
Baggage Claim Area	Space normally located in the passenger terminal building, where passengers reclaim checked baggage.
Baggage Makeup Area	Space in which arriving and departing baggage is sorted and routed to appropriate destinations.
BAP	Blast Analysis Plan
BHS	Baggage Handling System
BIDS	Baggage Information Display Systems
BMA	Baggage Makeup Area
Boarding Gate	The area from which passengers directly enplane or deplane the aircraft.
Cargo	Property tendered for air transportation accounted for on an air waybill. All accompanied commercial courier consignments, whether or not accounted for on an air waybill, are also classified as cargo. Any property carried on an aircraft other than mail, stores and accompanied or mishandled baggage. Aircraft operator security programs further define the term "cargo."
Cargo Area	All the ground space and facilities provided for cargo handling. It includes airport ramps, cargo buildings and warehouses, parking lots and roads associated therewith.
Carry-on baggage	An individual's personal property that is carried into a designated sterile area or into an aircraft cabin and is accessible to an individual during flight
CBP	Customs and Border Protection (U.S.)
CBRN	Chemical, Biological, Radiological, Nuclear
CBW	Chemical and Biological Weapon (or Chemical and Biological Warfare)
CCD	Charge-coupled Device
CCTV	Closed Circuit Television (System)
CFR	Code of Federal Regulations (U.S.)
CHRC	Criminal History Records Check

Checked Baggage Property tendered by or on behalf of a passenger and accepted by an aircraft operator for transport, which is inaccessible to passengers during flight. Accompanied commercial courier consignments are not classified as checked baggage.

Chem-Bio Chemical and Biological

Concourse A passageway for persons between the principal terminal building waiting area and the structures leading to aircraft parking positions.

CP Command Post (typically, for purposes of this document, the Airport Emergency Command Post)

CPU Central Processing Unit

Crisis Management Team A group of individuals involved in managing a crisis to prevent, or at least contain, a crisis situation from escalating, jeopardizing safety and facilities, attracting unfavorable attention, inhibiting normal operations, creating a negative public image, and adversely affecting the organization’s viability.

Curbside Check-in An area normally located along terminal’s vehicle curb frontage where designated employees accept and check-in baggage from departing passengers. Designed to speed passenger movement by separating baggage handling from other ticket counter and gate activities. Allows baggage to be consolidated and moved to the screening process and to the aircraft more directly.

CUPPS Common-Use Passenger Processing Systems

DHS The Department of Homeland Security (U.S.) and any directorate, bureau, or other component within the Department of Homeland Security, including the Transportation Security Administration.

DOT The Department of Transportation (U.S.) and any operating administration, entity, or office within the Department of Transportation.

DVR Digital Video Recorder

EDS Explosives Detection System

EIA Electronics Industry Alliance

Emergency Command Post A room or combination of rooms/facilities from which a Crisis Management Team commands and directs an event or incident such as a natural disaster, terrorist event, hostage situation or aircraft disaster.

EMS Emergency Medical Services

EOC Emergency Operations Center (See also Emergency Command Post

EOD Explosive Ordnance Disposal—To render safe either improvised or manufactured explosive devices by the use of technically trained and equipped personnel.

EBSP Electronic Baggage Screening Program

Escort To accompany or monitor the activities of an individual who does not have unescorted access authority into or within a secured area or SIDA

ETD Explosives Trace Detection (or Detector)

ETD In the context of passenger scheduling, ETD means “estimated time of departure.”

Exclusive Area Any portion of a secured area, AOA, or SIDA, including individual access points, for which an aircraft operator or foreign air carrier that has a security program under 49 CFR 1544 or 49 CFR 1546 has assumed responsibility under 49 CFR 1542.111.

Exclusive Area Agreement An agreement between the airport operator and an aircraft operator that permits the operator to assume responsibility for specified security measures in 49 CFR 1542.111. Does not include law enforcement responsibilities.

Explosives Military, commercial, or improvised compounds characterized by their ability to rapidly convert from a solid or liquid state into a hot gaseous compound with a much greater volume than the substances from which they are generated.

Explosives Detection System A system designed to detect the chemical signature of explosive materials, where the TSA has tested the system or devices against pre-established standards, and has certified that the system meets the criteria in terms of detection capabilities and throughput to detect in checked baggage, the amounts, types, and configurations of explosive materials as specified by TSA.

Explosives Trace Detection A device that has been certified by TSA for detecting explosive particles on objects intended to be carried into the sterile area or transported on board an aircraft. As used in this document, a device that detects tiny amounts of particle and/or vapor forms of explosives.

FAA Federal Aviation Administration (U.S.)

FAR Federal Aviation Regulation (U.S.)

FBO Fixed Base Operator

fc Footcandle

FCC Federal Communications Commission (U.S.)

FEMA Federal Emergency Management Agency (U.S.)

FIDS Flight Information Display Systems

FIS Federal Inspection Services (U.S.)—U.S. Customs and Border Protection (CBP), U.S. Fish and Wildlife Service (FWS), and Public Health Service (PHS)

FSD TSA Federal Security Director

GA General Aviation

General Aviation That portion of civil aviation that encompasses all facets of aviation except commercial and military aircraft operators.

Ground Transportation Staging Area [GTSA] The location where taxis, limos, buses and/or other ground transportation vehicles are staged prior to the terminal.

Hazardous Material As defined in 49 USC 5103 of the hazardous materials transportation law. Substances determined to be capable of posing an unreasonable risk to health, safety, and property when transported in commerce—also referred to as "dangerous goods" under international regulations.

Hijacking The exercising, or attempt to exercise, control over the movement of an aircraft by the use of force or threats, which if successfully carried out, would result in the deviation of an aircraft from its regularly scheduled route.

HVAC Heating, Ventilation and Air Cooling

IATA International Air Transport Association

ICAO International Civil Aviation Organization—a specialized agency of the United Nations whose objective is to develop the principles and techniques of international air navigation and to foster planning and development of international civil air transport.

ICE DHS Immigration and Customs Enforcement

ID Identification—use of methods such as access media, signs or markers to identify persons, vehicles and/or property

IED Improvised Explosive Device

IEEE Institute of Electrical and Electronic Engineers

IESNA Illumination Engineering Society of North America

IETF Internet Engineering Task Force

Improvised Explosive Device A device that has been fabricated in an improvised manner and incorporates explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals in its design. Generally an IED will consist of an explosive, a power supply, a switch or timer, and a detonator or initiator.

Incendiary Any substance that can cause a fire by ignition (flammable liquids, gases, or chemical compounds), or device that can be used to initiate a fire.

Indirect Air Carrier Any person or entity that undertakes to engage indirectly in air transportation of property, and uses the services of a passenger air carrier. This does not include the United States Postal Service (USPS) or its representative while acting on the behalf of the USPS.

Indirect Air Carrier Standard Security Program (ICASSP) A standard security program for indirect air carriers regulated in accordance with 49 CFR 1548

Intermodal The use of two or more modes of transportation to complete the movement of a passenger or cargo from origin to destination; for example, cruise ship-to-aircraft (passenger), or aircraft-to-truck-to-rail-to-ship (cargo).

International Airport An airport used as 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

IR Infrared

ISO International Standards Organization

Isolated Parking Position An area designated for the parking of aircraft suspected of carrying explosives or incendiaries to accommodate responding law enforcement and/or EOD personnel in search efforts.

IT Information Technology

ITU International Telecommunications Union

K-9 Canine Team—Dog teams used for explosives or other material detection.

kg Kilogram, 1000 grams or 2.2 pounds (a typical spray can holds approximately 300 grams)

LAN Local Area Network

Law Enforcement Officer An individual authorized to carry and use firearms, vested with such police power of arrest as determined by Federal Law and State Statutes, and identifiable by appropriate indicia of authority, and who is trained and commissioned to enforce the public criminal laws of the jurisdiction(s) in which he or she is commissioned.

Landside That area of an airport and buildings to which both traveling passengers and the non-traveling public have unrestricted access. (See also Non-restricted area.)

LED Light-Emitting Diode

LEO Law Enforcement Officer

LVIED Large Vehicle IED

Metal Detector
[also: “magnetometer”] An electronic detection device approved by the TSA to detect metal on persons desiring access beyond the screening point. May be walk-through or hand-held type.

micron 0.001 Millimeter or 0.00004 inches

Movement Area The runways, taxiways, and other areas of an airport used for taxiing, takeoff, and landing of aircraft, exclusive of loading ramps and aircraft parking areas.

NAS Network Attached Storage

NEC National Electrical Code

NFPA National Fire Protection Association (U.S.)

NIST National Institute of Standards and Technology (U.S.)

Off-Airport Facility Refers to a passenger or cargo transport terminal at an urban population center at which processing facilities are provided prior to arrival at airport.

On-Screen Alarm Resolution EDS tools/functions that can be used to resolve or suspect EDS alarm objects

Perimeter The outer boundary of an airport, also a boundary that can separate areas controlled for security purposes from those that are not.

Person An individual, corporation, company, association, firm, partnership, society, joint-stock company, or governmental authority. It includes a trustee, receiver, assignee, successor, or similar representative of any of them.

PIN Personal Identification Number

POE Port-of-Entry (FIS).

Private Charter Any aircraft operator flight—(1) For which the charterer engages the total passenger capacity of the aircraft for the carriage of passengers; the passengers are invited by the charterer; the cost of the flight is borne entirely by the charterer and not directly or indirectly by any individual passenger; and the flight is not advertised to the public, in any way, to solicit passengers; (2) For which the total passenger capacity of the aircraft is used for the purpose of civilian or military air movement conducted under contract with the Government of the United States or the government of a foreign country

PTZ Pan/Tilt/Zoom

Public Area That portion of the airport which includes all public real estate and facilities other than the air operations area and those sterile areas downstream of security screening stations

RAID Redundant Array of Independent Disks

Record Includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term record also includes any draft, proposed, or recommended change to any record.

RF Radio Frequency

RFI Radio Frequency Interference

RFID Radio Frequency Identification

RTCA Radio Technical Commission for Aeronautics

SAN Storage Area Network

SARP Standards and Recommended Practices (ICAO)

Screening The application of technical or other means which are intended to identify and/or detect weapons, explosives or other dangerous devices, articles or substances which may be used to commit an act of unlawful interference. The checked baggage screening functions are: (1) EDS screening, (2) ETD screening, (3) combination of EDS/ETD, and (4) physical inspection.

Screening Location Each site at which individuals, accessible property, or checked baggage is inspected for the presence of explosives, incendiaries, weapons, or other prohibited items. These include the screening checkpoint or boarding gate where individuals and accessible property are inspected with metal detectors, X-ray devices, and other methods; concourse, lobby or baggage make-up areas where checked baggage is inspected with an EDS and/or ETD; and locations where cargo is inspected.

Secured Area A portion of an airport, specified in the 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.

Security Areas Areas defined by and subject to security requirements and regulation; e.g., AOA, ATSP Area, Exclusive Use Area, Secured Area, SIDA, Sterile Area

Security Contingency Plan A plan detailing response procedures to address a transportation security incident, threat assessment, or specific threat against transportation, including details of preparation, response, mitigation, recovery, and reconstitution procedures, continuity of government, continuity of transportation operations, and crisis management

Security Directive A document issued by TSA to notify aircraft operators and/or airport operators of specific credible threats, and measures required for response.

Security Identification Display Area [SIDA] A portion of an airport, specified in the 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 A program or plan and any amendments, developed for the security of (1) An airport, aircraft, or aviation cargo operation; (2) A maritime facility, vessel, or port area; or (3) A transportation-related automated system or network for information processing, control, and communications.

Security Parking Area An aircraft stand where aircraft threatened with unlawful interference may be parked pending resolution of the threat. Also known as “hot spot.”

Shield Alarm An EDS alarm caused by substances too dense for X-rays to penetrate and which EDS is unable to analyze

Should For the purpose of this document, this word is defined as a recommendation or that which is advised but not required.

SIDA Security Identification Display Area

SOC Security Operations Center

SONET Synchronous Optical Network

SSCP Security Screening Checkpoint—A checkpoint area established to conduct security screening of persons and their possessions prior to their entering a sterile or secured area.

SSI Sensitive Security Information, as described in 49 CFR §1520.5

Stand-Alone Systems A non-integrated checked baggage screening system where the passenger checks his or her baggage with the aircraft operator in the airport lobby for screening by an EDS and/or ETD

Sterile Area A portion of an airport defined in the 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 or a foreign air carrier, through the screening of persons and property. Generally, that area between passenger screening checkpoint and the aircraft boarding areas.

TCU Threat Containment Unit—a wide variety of devices used to contain wholly or in part the blast effects of an explosive device. TCUs may be stationary, or may be part of a system by which an explosive device may be transported.

Terminal A building or buildings designed to accommodate the enplaning and deplaning activities of aircraft operator passengers.

Threat A threat is any indication, circumstance or event with the potential to cause loss of or damage to an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to 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.

Through the Fence Agreement Allows an off-airport aircraft owner at an off-airport property to use a cross - boundary taxiway to access the airport's taxiway-runway system.

Transportation Security Regulation(s) The regulations issued by the Transportation Security Administration, in Title 49 of the Code of Federal Regulations, Chapter XII, which includes parts 1500 through 1699.

TSA Transportation Security Administration (U.S.)

TSNM Transportation Sector Network Management (TSA)

TTAC Transportation Threat Assessment and Credentialing (TSA)

Unescorted Access Authority The authority granted by an airport operator, an aircraft operator, foreign air carrier, or airport tenant under part 1542, 1544, or 1546, to individuals to gain entry to, and be present without an escort in, secured areas and SIDAs of airports

UPS Uninterruptible Power Supply

VLAN Virtual Local Area Network

Vulnerability A weakness in physical structures, personnel protection systems, process or other areas that may be exploited by criminals or terrorists

Vulnerability Assessment Any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, vessel, aircraft, train, commercial motor vehicle, or pipeline, or a transportation-related automated system or network, to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A vulnerability assessment may include proposed, recommended, or directed actions or countermeasures to address security concerns.

Vulnerable Area / Point Any facility or area at an airport, which, if damaged or otherwise rendered inoperative, would seriously impair the functioning of an airport.

VPN Virtual Private Network

WAN Wide-Area Network

WLAN Wireless Local Area Network

WMD Weapons of Mass Destruction (typically includes chemical, biological, radiological, and nuclear weapons)

WTMD Walk-Through Metal Detector

APPENDIX H
BIBLIOGRAPHY

Note

DHS, TSA, FAA and other sources/agencies listed below periodically update many of the documents, rules, regulations, statutes and codes referenced in this bibliography. These updates sometimes change the entire document, but more often the changes are only in segments as new information becomes available. The reader should seek guidance directly from the source to ensure the referenced document is the most the most current version.

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 http://www.faa.gov/regulations_policies/advisory_circulars/ for an index of all circulars; the series of A/Cs designated "150" applies to airports. Additional contact names and numbers may also be found there.

1. 00-2, Advisory Circular Checklist—Contains a listing of all current 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. 150/5200-31C (June 19, 2009) Airport Emergency Plan (Consolidated AC includes Change 2)
4. 150/5300-13, Airport Design
5. 150/5360-13, Planning and Design Guidelines for Airport Terminal Facilities. Furnishes guidance material for the planning and design of airport terminal buildings and related facilities.
6. 150/5370-10, Standards for Specifying Construction of Airports

Section B—Government Reports and Regulations

Government reports may be obtained from the National Technical Information Services (NTIS), 5301 Shawnee Road, Alexandria, VA 22312; Tel: (703) 605-6040 (http://www.ntis.gov/).

Most reports may also be obtained directly from the originating government agency and are often also available on the agency's Internet Web site.

1. Aviation and Transportation Security Act (ATSA). Public Law 107-71. 115 Statute 597.
http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf
2. 49 CFR 1520. Protection of Sensitive Security Information
3. 49 CFR 1540. Civil Aviation Security General Requirements.
4. 49 CFR 1542. Airport Security.
5. 49 CFR 1544. Aircraft Operator Security.
6. 49 CFR 1546. Foreign Air Carrier Security.
7. 49 CFR 1548. Indirect Air Carrier Security.
8. 14CFR139. Certification and Operations: Land Airports Serving Certain Air Carriers

9. 14 CFR 139.325—Airport emergency plan.

10. Homeland Security Act, Public Law 107-296. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ296.107.pdf

11. Planning Guidelines and Design Standards (PGDS) for Checked Baggage Inspection Systems (CBISs), TSA. The PGDS is updated annually and can be accessed at: http://www.tsa.gov/research/checked_baggage_material.shtm .

12. Electronic Baggage Screening Program (EBSP). Guidance and sample documentation will continue to be reviewed, updated and posted to: http://www.tsa.gov/research/checked_baggage_material.shtm under In-Line Support Application Documents.

13. National Incident Management System, December 2008, United States Department of Homeland Security, http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf

14. TSA NEDCTP Canine Training & Evaluations Branch, TSA K-9 Contact Information http://www.tsa.gov/lawenforcement/programs/editorial_multi_image_0002.shtm

15. Chemical & Biological Agent Resources and guidance may be obtained from TSA, Federal Emergency Management Agency (FEMA), Federal Bureau of Investigation (FBI), Department of Energy (DOE), Center for Disease Control (CDC)

16. U.S. DHS, Transportation Security Administration security regulations

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. Some publications are free and others available for purchase.)

1. Airport Planning Manual—Master Planning, Part 1 (Doc 9184). International Civil Aviation Organization. www.icao.int (available for purchase)

2. Transit Security Design Considerations, Final Report, John A. Volpe National Transportation Systems Center, U.S. Department of Transportation, November 2004.

3. DoD Minimum Antiterrorism Standards for Buildings, U.S. Department of Defense, October 2003 (including change 1, 19 January 2007) and the National Institute of Building Sciences (http://www.wbdg.org/)

4. Physical Security. U.S. Army FM 3.19.30, January 2001.

5. 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

6. Guidelines to Improve Airport Preparedness Against Chemical and Biological Terrorism, Edwards, Dr. Donna M., et al, Sandia Berkley National Laboratory, Albuquerque, New Mexico 87185 and Livermore, California 94550. SAND2005-3237/LBNL-54973 (II), May 2005, prepared for the U.S. Department of Energy.

7. Glazing Hazard Mitigation, by Joseph L. Smith, PSP and Nancy A. Renfroe, PSP, Applied Research Associates, Inc., http://www.wbdg.org/resources/glazingmitigation.php

8. Building Security: Handbook for Architectural Planning and Design, Barbara A. Nadel, published by McGraw-Hill Professional, April 2004. Available for purchase from Internet book sites.

9. International Standards and Recommended Practices—Security—Aerodromes—Annex 14 to the Convention on International Civil Aviation. Volume I, Aerodrome Design and Operations. International Civil Aviation Organization. Available for purchase from: http://www.icao.int/

10. International Civil Aviation Organization—Standards and Recommended Practices—Security—Safeguarding International Civil Aviation Against Acts of Unlawful Interference—Annex 17 to the Convention on International Civil Aviation. Available for purchase from: http://www2.icao.int/en/avsec/pages/default.aspx/

11. International Civil Aviation Organization—Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference (Doc 8973, restricted distribution). International Civil Aviation Organization. Available for purchase from ICAO. http://www2.icao.int/en/avsec/pages/default.aspx/

12. National Fire Codes NFPA 101—Life Safety Code. National Fire Prevention Association. Available for purchase from www.nfpa.org:

13. National Fire Codes NFPA 415—Standard on Construction and Protection of Airport Terminal Buildings, Fueling Ramp Drainage, and Loading Walkways, 2008 Edition, National Fire Prevention Association. Available for purchase from: www.nfpa.org

14. Merritt Risk Management Manual, available for purchase from Silver Lake Publishing at: www.riskmanagementmanual.com/index.php

15. RTCA/DO-230C, Standards for Airport Security Access Control Systems (approx. publishing date is June 2011. Previous version 230B is available.). http://www.rtca.org/doclist.asp Publications are available for purchase.

16. RTCA/DO-221, Guidance and Recommended Requirements for Airport Surface Movement Sensors (1994), http://www.rtca.org/doclist.asp Available for purchase.

17. Security Guidelines for General Aviation Airports. Aviation Security Advisory Committee. (2004) http://www.tsa.gov/assets/pdf/security_guidelines_for_general_aviation_airports.pdf This publication is being updated in 2011.

18. Terrorism in the United States—Terrorist Research and Analytical Center. Counter Terrorism Section, Criminal Investigative Division. Federal Bureau of Investigation. Annual.

19. Terrorism reports, http://www.fbi.gov/stats-services/publications

20. Vulnerability Identification Self Assessment Tools (Hazmat Risk Assessment and Vulnerability Evaluation; Port and Intermodal Vulnerability Identification Self-Assessment; and Mass Transit Vulnerability Identification Self-Assessment), Transportation Security Administration, U.S. Department of Homeland Security http://www.tsa.gov/what_we_do/risk/editorial_0824.shtm

21. DOE Vulnerability and Risk-Assessment Methodology, Vulnerability and Risk Management Program, U.S. Department of Energy, 2001 (Available through the Electricity Sector—Information Sharing and Analysis Center (ESISAC) www.esisac.com/publicdocs/assessment_methods/AppD_DOE_VRAP.pdf

22. Lessons Learned from Industry Vulnerability Assessments and September 11th, a presentation of Argonne National Laboratory, U.S. Department of Energy, December 2001 http://www.naseo.org/committees/energysecurity/archive/meetings/2001-12-12/stern.pdf

23. 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

24. A How-To Guide Mitigate Potential Terrorist Attacks Against Buildings, FEMA 452, January 2005, Federal Emergency Management Agency, U.S. Department of Homeland Security http://www.fema.gov/library/viewRecord.do?id=1938 (Available for download, free)

25. Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks, FEMA 427, December 2003, Federal Emergency Management Agency, U.S. Department of Homeland Security http://www.fema.gov/plan/prevent/rms/rmsp427

26. Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, FEMA 426, December 2003, Federal Emergency Management Agency, U.S. Department of Homeland Security http://www.fema.gov/library/viewRecord.do?id=1559

27. *The Design and Evaluation of Physical Protection Systems*, Mary Lynn Garcia, published by Butterworth-Heinemann, 2001. Available for purchase at Internet book sites.

28. Progressive Collapse Analysis and Design Guidelines for New Federal Office Buildings and Major Modernization Projects, (U.S. General Services Administration, June 2003)

http://www.cement.org/buildings/US-GSA-ProgCollapse-SEI-04.pdf GSA, 08-Security Design http://www.gsa.gov/portal/category/21057

29. 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/main-pub.cfm?usr=clfma

30. TSA Checkpoint Design Guide (CDG), Revision 1, February 11, 2009 http://www.aci-na.org/static/entransit/OPT%20%20Checkpoint%20Design%20Guide%20%28CDG%29%202009.pdf

31. TSA Security Checkpoint Layout Design (2006) http://www.aci-na.org/static/entransit/Checkpoint_Layout_Design_Guide_v1r0-0.pdf

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) http://www.uscis.gov/portal/site/uscis/ilink/?vgnextchannel=fa7e539dc4bed010VgnVCM1000000ecd190aRCRD&SC=/ilink/docView/SLB/HTML/SLB/0-0-0-1/0-0-0-29/0-0-0-5361.html 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. http://www.uscis.gov/ilink/docView/SLB/HTML/SLB/0-0-0-1/0-0-0-11261/0-0-0-22435/0-0-0-22459.html#0-0-0-14953

3. Presidential Decision Directives. www.fas.org/irp/offdocs/nspd/index.html

   The Presidential Decision Directive (PDD) series is used to promulgate Presidential decisions on national security matters.

   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. http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm

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. http://dhsprojects.com/SAS-DO-SO/CBPAirportTechnicalDesignStandards.pdf

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/

Section E—Miscellaneous Regulations, Reports, and Resources

1. FAA Circular 150/5360-12E (http://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/74209), updated June 2010 recommends the use of these Guidelines for designing airport terminal signing systems

2. U.S. Department of Justice Americans with Disabilities Act (ADA) for regulatory requirements and guidance. http://www.ada.gov/2010ADAstandards_index.htm

3. Ergonomic and workplace standards and requirements of the U.S. Department of Labor Occupational Safety & Health Administration (OSHA) are available at the following Web sites:
   www.osha.gov/SLTC/ergonomics
   www.osha.gov/SLTC/etools/baggagehandling/index.html
   http://www.osha.gov/SLTC/etools/computerworkstations/components_monitors.html

4. ASTM F2656—07 Standard Test Method for Vehicle Crash Testing of Perimeter Barriers, American Society for Testing and Materials (ASTM), http://www.astm.org/Standards/F2656.htm

5. IEEE802, IEEE 802 LAN/MAN Standards Committee, http://www.ieee802.org/

6. Personal Identity Verification (PIV) of Federal workers and contractors,
   http://csrc.nist.gov/groups/SNS/piv/index.html
   http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
   http://csrc.nist.gov/publications/nistpubs/800-79-1/SP800-79-1.pdf

7. International Building Code Council, http://www.iccsafe.org/Pages/default.aspx

8. Building Industry Consulting Service International, Inc., BICSI, https://www.bicsi.org/default.aspx

9. National Electric Code, NEC, http://www.neccodebooks.com/

10. Telecommunications Industry Association (TIA), http://www.tiaonline.org/
    "Administrative Standard for Telecommunications Infrastructure," TIA/EIA-606A,
    http://standardsdocuments.tiaonline.org/tia-606-a.htm

11. Electronic Industry Alliance (EIA). EIA ceased operations in Dec 2010. EIA Standards are managed by ECA, http://ec-central.org/index.cfm

12. American National Standards Institute (ANSI), http://www.ansi.org/

13. ANSI/IESNA RP-104, ANSI Standards Store

13. NIST Risk Management Framework (RMF), http://csrc.nist.gov/groups/SMA/fisma/framework.html
    NIST 800-53 "controls," http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

14. American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE), http://www.ashrae.org/

15. National Emergency Number Association, NENA Master Glossary of 9-1-1 Terminology, http://www.nena.org

16. IATA, The Airport Development Reference Manual (ADRM)

17. National Safe Skies Alliance

18. Common Use Passenger Processing Systems (CUPPS)

19. Institute of Electrical and Electronic Engineers (IEEE)

20. Internet Engineering Task Force (IETF)

21. International Telecommunications Union (ITU)

22. The International Organization for Standardization (ISO)

23. Federal Communication Commission (FCC)

24. The Critical Infrastructure Key Resource (CIKR) Annex

25. National Transportation Safety Board

Section F—Additional References for Part III, Section H, Video Surveillance, Detection and Distribution Systems

1. “Defining Video Quality Requirements: A Guide for Public Safety, Version 1.0,” developed by the Video Quality in Public Safety Group under sponsorship of the U.S. Department of Homeland Security Office of Interoperability and Compatibility (OIC), and the U.S. Department of Commerce Public Safety Communications Research (PSCR) program, Washington D.C. (2010) http://www.safecomprogram.gov/NR/rdonlyres/5BCA1CBF-1500-4B29-9370-81B823575DE8/0/3aVideoUserRequirementGuidedoc.pdf

2. “The Target Task Performance (TTP) Metric: A New Model for Predicting Target Acquisition Performance,” Technical Report AMSEWL-NV-TR-230, U.S. Army CERDEC, Ft. Belvoir VA (2004) http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA422493&Location=U2&doc=GetTRDoc.pdf

3. “New Metric for Predicting Target Acquisition Performance,” R. Vollmerhausen et al, Optical Engineering (43)11, pp. 2806-2818 (2004) http://lib.semi.ac.cn:8080/tsh/dzzy/wsqk/SPIE/vol5076/5076-28.pdf

4. “RFC 2326: The Real Time Streaming Protocol (RTSP),” the Internet Engineering Task Force (IETF) (1998) http://www.ietf.org/rfc/rfc2326.txt

5. “Electro-Optical System Design, Analysis, and Testing,” M. Dudzik, Ed., in “The Infrared and Electro-Optical System Handbook, Vol. 4,” Environment Research Institute of Michigan, Ann Arbor MI (1993) http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA364024&Location=U2&doc=GetTRDoc.pdf

6. “Modeling target acquisition tasks associated with security and surveillance”; Vollmerhausen and Robinson, Applied Optics, Vol. 46, Issue 20, pp. 4209-4221 (2007) http://www.opticsinfobase.org/abstract.cfm?uri=ao-46-20-4209