Section 01555
Airport Security Construction Requirements

City of Austin
Department of Aviation
Austin-Bergstrom International Airport

Issue Date:
March 31, 2022

Airport Construction Security Requirements – Section 01555

Table of Contents:

Table of Contents (Continued, page 2)

Table of Contents (Continued, page 3)

Table of Contents (Continued, page 4)

1. Introduction

This document (hereinafter referred to as "Section 01555 - Construction Security Guidelines" or "guidelines") is a guide to security standards that all operators, tenants, vendors and others responsible for construction, operation, and/or maintenance of space on/within the grounds of the Austin-Bergstrom International Airport (AUS) will be required to incorporate into the development and management of AUS facilities. Section 01555 – Construction Security Guidelines serves to supplement other policies and procedures used by AUS staff to ensure the Airport complies with existing federal requirements and AUS security standards. While these guidelines help reduce risk, they cannot eliminate it and all persons maintain individual responsibility for ensuring compliance with federal and local requirements regardless of whether or not stated in within these guidelines. AUS reserves the right to correct any clerical errors within this guideline and impose additional measures not stated within these guidelines as required to maintain a safe and secure operation and comply with local, state, and federal regulations. All persons maintain individual responsibility for meeting reasonable standards of care and compliance associated with their activities and facilities.

1.1 Purpose

These guidelines serve as a supplementary guide to the physical security standards that have been established by AUS for the planning, design, construction, operation and maintenance of AUS facilities. These guidelines include guidance issued by the United States Department of Homeland Security's, Transportation Security Administration (TSA) and Cybersecurity and Critical Infrastructure Security Agency (CISA); the United States Department of Transportation, Federal Aviation Administration (FAA); industry best security practices; and, AUS requirements for the safe and secure planning, design, construction, operation and maintenance of facilities, sites and spaces on the airport. These security guidelines are intended to inform persons of security considerations to be addressed in accordance with applicable security policies, guidelines, laws, and regulations.

1.2 Applicability

These guidelines will be incorporated into all new construction design approvals, design approvals for changes to any existing facilities, and new AUS agreements and renewals. For alteration, renovation and/or modification activities to existing premises, unless the intended use of the premises is to be changed, the applicability of the requirements shall be proportionate and commensurate with the nature of such alteration, renovation, and/or modification as determined by AUS. If the intended or actual use of an existing premises is changed, AUS may deem any and all applicable requirements of the guidelines to be applied. Any deviation from these guidelines, must be approved by an authorized AUS security official.

1.3 Inspections

AUS may conduct surveys of spaces/facilities at any time prior to, during and after construction or an alteration, or during occupancy to ensure the guidelines are satisfied. Access means for routine inspections and/or real-time emergency access must be provided in a manner approved by AUS tenant management, planning and development, and security personnel. Areas under TSA regulatory oversight are also subject to unannounced inspections by AUS Security Compliance and/or TSA Transportation Security Inspectors.

2. Project Security Communication

Communication regarding project security shall be routed through below listed representatives so as to provide clear, consistent, and documentable relay of information.

2.1 Tenant Representatives

2.1.1 Authorized Signatory is a designated representative of the tenant to receive all communications regarding security regulatory requirements, including employee access/identification media issuance described in section 11. All security communications between the tenant and AUS Airport Security should be routed through the authorized signatory unless a supplementary Contractor Security Coordinator is identified for the project.

2.1.2 Contractor Security Coordinator serves as the contractor provided designated representative for security communications with AUS specific to a project. A contractor security coordinator may also be designated by a tenant to co-serve as an authorized signatory for employee access/identification media issuance. A contractor security coordinator may be deemed unfit to fulfill his/her duties by AUS, which will require a suitable replacement be assigned by the contractor. Failure to maintain a suitable contractor security coordinator will result in revocation of all AUS issued access/identification media for the contractor and denial of access to any AUS restricted areas.

2.2 AUS Representatives listing will be provided on a project-to-project basis. Lists of below listed AUS personnel shall be treated as Confidential Privileged Information (CPI) and shall not be included in publically available materials.

2.2.1 AUS Project Manager manages design and building of Airport Capital Improvement Projects and co-manages design and construction of airport tenant and third party project. Coordinates projects with Airport workgroups/operations. Issues Notice to Proceed approval for projects.

2.2.2 AUS Tenant Manager Representative acts as a liaison to airport tenants, concessionaires, airlines, and other stakeholders. The Tenant Manager Representative receives and processes Tenant Project – Concept Proposal Information Sheet (CPIS) forms in the submission process for tenant projects.

2.2.3 AUS Airport Security

2.2.3.1 Airport Security Manager
Airport Security Manager (ASM) is the primary contact for compliance with security regulations. The ASM reviews plans and advises on security requirements. The ASM serves as liaison with the Austin Police Department, DHS TSA, CISA, CBP and DOJ FBI regarding airport security.

2.2.3.2 Airport Security Coordinator (ASC) serves as the subject matter expert for the assigned aspects of airport security: security plan, worker vetting and badging, access control, tenant compliance, and physical security.

2.3 Emergency Communication should be routed through the Airport Operations Center which is staffed 24/7 – the center may be contacted at 512-530-2242(ABIA).

3. Access requirements for certain airport areas.

3.1 Security classification. In general there are two broad security classifications of airport areas: non-restricted areas and restricted areas.

3.1.1. Non-restricted areas are any portions of the Airport campus designed to be accessible to general public or otherwise not falling under the description of a sterile area, secured area, air operations area, or identified as a security identification display area. Primary security concerns in these areas are: minimizing the potential for mass casualty events by limiting or mitigating congregation areas; providing blast protection; providing for adequate surveillance and emergency response access; and, providing adequate barriers to adjacent restricted areas. Examples of non-restricted areas located within AUS are: hotels and convenience stores, public roadways and parking structures, AUS administration and support facilities, and airline ticketing/check-in counters and baggage claim portions of terminals.

3.1.2. Restricted areas are those portions of the Airport campus to which access is restricted under governing federal and/or local regulations. These areas may be further classified as: air operations area (**AOA**), **secured area**, security identification display area (**SIDA**), and **sterile areas** – all having the meanings as defined in US 49 CFR 1540.5. In addition to the security concerns of non-restricted areas, restricted areas also have specific regulatory security requirements that may vary to each classification and location on AUS. Access to AUS restricted areas may be controlled through the automated access control system, manual access control (lock and key), and/or posted markings or signage. Vehicles and persons within and/or disturbing existing barriers of AUS restricted areas are subject to the access and identification media requirements described within section 11 of this guide.

3.2 Landside areas of AUS are classified as non-restricted areas; however, special attention is required in landside areas immediately adjacent to restricted areas and within 300’ of any portion of terminals. Access to some landside areas may also be controlled through the automated access control system or manual access controls, vehicles and persons within such areas may be subject to the access and identification media requirements described within section 11 of this guide as determined by the Airport Security Manager (examples of such controlled areas include “De-Icing Ponds” and the “Central [Utility] Plant”).

3.3 Airside areas of AUS are all classified as restricted areas and further classified as either: AOA, secured areas, or SIDAs. Vehicles and persons within and/or disturbing existing barriers of AUS restricted areas are subject to the access and identification media requirements described within section 11 of this guide.

3.4 Terminals at AUS consist of both restricted and non-restricted areas. The boundary between such areas is separated by physical barriers such as walls, automated or manual access control portals, or staffed portals (passenger screening checkpoints and sterile area passenger exits). In addition to the access and identification media requirements described within section 11 of this guide for accessing restricted areas, additional requirements may be required for work within the following areas of terminals:

3.4.1. Sterile areas of the terminal are portions to which access is under the direct regulatory control of TSA through the passenger process. Employees and all items in their possession must either enter the sterile area through the passenger screening process or use an AUS identified alternate route. In addition to the access and identification media requirements described within section 11 of this guide for restricted area access, all persons and all items

in their possessions are subject to search/inspection by AUS and TSA personnel. When accessing the sterile area through the passenger screening process, no TSA deemed "prohibited items" (those items identified as being prohibited from carry-on bags at: https://www.tsa.gov/travel/security-screening/whatcanibring/all) may be possessed. When accessing the sterile area through an AUS identified alternate route, only those TSA deemed "prohibited items" to which an employee has an articulable and demonstrable business need may be possessed. ***Alternate access routes may not be used if accessing the sterile area to travel as a passenger or crew of an aircraft – all such entry of persons and items must be made through the passenger screening process.**

3.4.2. Transportation Security Administration (TSA) offices and equipment. Work within TSA leased portions of the terminal or work which will affect the operation of TSA screening equipment and/or spaces shall be coordinated/approved through the TSA Federal Security Director. Work within these areas are affecting screening equipment and/or spaces should be coordinated at least 30 days in advance.

3.4.3. Federal Inspection Services (FIS) and Customs and Border Protection (CBP) offices. At the discretion of the CBP Port Director, work within the FIS and CBP offices may require acquisition of "Custom Seals" for personnel. Work within these areas must be coordinated at least 30 days in advance to allow for clearance through CBP processes, if required.

3.4.4. Austin Police Department (APD) offices. Systems within APD offices are subject to Texas Department of Public Safety, Criminal Justice Information Systems (CJIS) regulatory requirements. Work within these areas may require supervision/escort by APD personnel and shall be coordinated/approved through the APD Airport Division command. Work within APD offices should be coordinated at least 30 business days in advance.

3.4.5. Airport Operations Center (AOC). Systems within the AOC are subject to Texas Department of Public Safety, Criminal Justice Information Systems (CJIS) regulatory requirements. Work within these areas may require supervision/escort by AUS personnel. Work within the AOC must be coordinated at least 3 business days in advance.

3.4.6. Terminal electrical rooms, mechanical rooms, and rooftops. Access to terminal electrical and mechanical rooms and the terminal rooftop is at the discretion of the AUS Maintenance Manager. Work within these areas may require supervision/escort by AUS Maintenance Personnel. Work within these areas must be coordinated at least 3 business days in advance.

3.4.7. Terminal telecommunication/IT rooms. Access to terminal telecommunication/IT rooms is at the discretion of the AUS Information Systems Manager. Work within these areas may require supervision/escort by AUS Information Systems personnel. Work within these areas must be coordinated at least 3 business days in advance.

4. General Project Security Requirements

4.1 General security design considerations. Projects shall utilize an experienced planner/designer, with demonstrable like experience, whom shall incorporate measures consistent with the latest version of the TSA - Recommended Security Guidelines for Airport Planning Design and Construction, PARAS 0004 - Recommended Security Guidelines for Airport Planning, Design and Construction, (both of the afore mentioned are available through industry organizations such as Airport Consultants Council and Safe Skies) and any applicable regulatory requirements. When any potential conflict of such resources, any other airport planning standards, or these guidelines exists, the Airport Security Manager shall be consulted for determination of required measures and/or actions.

4.2. Security consultant required. Project planners/designers of facilities subject to regulatory requirements under CFR 49 Parts 1500-1548 must utilize a qualified and experienced security professional familiar with the threats and federal regulatory requirements specific to security category 1 or higher security categorized airports as applicable to the project scope. Demonstrable qualifying experience of this security professional shall be provided to the AUS Airport Security Manager for review/approval.

4.3. Notice to proceed. No alterations or modifications to any facility, structure, and/or area on the Airport may occur without a Notice to Proceed being issued by an authorized AUS representative. Airport Security shall be provided adequate opportunity to review all projects prior to issuance of the Notice to Proceed for purposes of any project security requirements.

4.4. Statement of intended use. To ensure required regulatory security elements are included, all projects must include clear statements of intent for which each area associated with the project will be used. The intended use of each area, including associated access routes/means, must be reviewed and approved by Airport Security. No changes to the intended use of an area or the associated access routes/means may occur without further review and approval through Airport Security.

4.5. Isolation of construction areas. To the extent possible, areas shall be transitioned to non-restricted areas or segregated from adjacent restricted areas through the use of approved barriers during the course of construction. Any changes/additions to restricted area barriers and/or access means must be submitted for security review at a minimum of 60 days in advance.

4.6. Addition and/or modification to access portals. At the discretion of Airport Security, any additions or changes to any restricted area access portals must be incorporated into the Airport's automated access control system (ACS) and monitoring under the Airport's CCTV system. Such additions/changes will be at the expense of the tenant and shall include associated licensing, data processing/storage, monitoring, and maintenance provisions. AUS Security and Operations personnel shall be consulted in planning and review stages and have final determination authority regarding required ACS and CCTV placements and utilizations. Systems information will be provided by AUS on a "need to know" basis.

Projects shall also be reviewed for potential of non-restricted to restricted area non-traditional portals that may require similar measures or other approved mitigation measures, all such potential portals must be clearly identifiable on submitted plans/drawings. Such non-traditional portals may include but are not limited to:

4.6.1. Windows within facilities serving as non-restricted to restricted area barriers or traversing separate areas defined under 49 CFR 1540.5;

4.6.2. Fire escapes/ escape routes within facilities serving as non-restricted to restricted area barriers;

4.6.3. Drainage culverts of greater than 8 inches in diameter or having openings greater than 60 square inches traversing non-restricted to restricted areas or separate areas defined under 49 CFR 1540.5;

4.6.4. Utility corridors of greater than 8 inches in diameter or having openings greater than 60 square inches traversing non-restricted to restricted areas or separate areas defined under 49 CFR 1540.5;

4.6.5. Maintenance chases and hatches within facilities serving as non-restricted to restricted area barriers, or traversing separate areas defined under 49 CFR 1540.5;

4.6.6 Ventilation ducting traversing non-restricted to restricted areas or separate areas defined under 49 CFR 1540.5;

4.6.7. Trash chutes traversing non-restricted to restricted areas or separate areas defined under 49 CFR 1540.5; and,

4.6.8. Frangible wall or barrier materials within facilities serving as non-restricted to restricted area barriers.

4.7. Airport automated Access Control System (ACS) and Closed Circuit Television (CCTV) systems. The Airport maintains monitored ACS and CCTV systems used for controlling and monitoring movement throughout security sensitive portions of the Airport. All projects must be evaluated by AUS Airport Security for required inclusion and/or potential impact upon these systems. Any additions, changes, or modifications required to ACS or CCTV systems will be at the expense of the tenant/project; and, shall include associated licensing, data processing/storage, monitoring, and maintenance provisions. All work on the ACS and CCTV systems shall be performed by qualified and licensed installers with integration performed only by the Airport's designated integrator. ACS placements shall include tamper mitigation measures including but not limited to: bezel tamper alarm reporting for reader or other trigger devices; locking and alarmed cabinets for controllers; all peripheral device connections shall be in EMT to controller box; and, all peripheral devices allowing ACS control to be overridden (such as gate motor control boxes) shall be alarmed and/or locked. AUS Security and Operations personnel shall be consulted in planning and review stages and have final determination authority regarding required placements and utilizations. Systems information will be provided by AUS on a "need to know" basis.

4.7.1. Restricted area ACS/CCTV portal requirements. At all portals providing non-restricted to restricted area access or transitioning from one type of restricted area (non AOA/Secured Area SIDA, AOA, Secured Area, or Sterile Ares) the following shall be included (any exception must be directly approved by the AUS Airport Security Manager):

- Provide badge in/badge out capabilities with each reader independently configurable within the ACS. Motion sensors, push buttons, vehicle sensors, and other similar devices that do not record system user information may not be used as access request devices.
- Include an audio and visual beacon/alarm to indicate "forced open" and "hold open" activities – a separate beacon/alarm is required for each pedestrian portal;
- Portals must include accommodations to support later inclusion to visual biometric systems – specifically each ACS placement shall have provision to receive an accompanying CCTV placement on the lowest security level side of the portal capable of viewing key identifying markers of access/identification media holders. CCTV placements provision should provide for cameras should be positioned with a vertical angle of approximately 45 degrees or more, and capable of providing an image of the ACS user from a height of 1 foot below and 3 feet above the ACS reader placement height.

4.8. Manual and/or tenant installed locking systems. Only use of the Airport's patented Best cores series (1C7 cores with 626 finish) may be installed in AUS owned facilities or areas housing AUS critical infrastructure (except for temporary locks used only during the construction period as described section 11.3). Use of Airport Best cores does not forego any requirements for portal integration into the Automated Access Control System as described in section 4.7. Contractors shall arrange for orders for locks and initial keys needed to be placed through a Best authorized representative. Contractor shall also coordinate any keying meetings with a Best representative to identify lock series architecture for facilities. The Airport will provide available series/subseries information to Best to facilitate the order. Core and key orders under the Airport's patented Best series shall be shipped directly to the Airport – cores will be installed by AUS personnel and keys will be issued by AUS personnel. At the request of company authorized signatories, the Airport Security and Identification Office will provide additional copies of keys to tenants outside of the project at the current fee as listed in the Security and Identification fee schedule – available to authorized signatories.

4.9. Confidential Privileged Information (CPI) and **Security Sensitive Information (SSI).** Any threat related information, including threat mitigation measures, that is generated in the planning, design, and construction processes shall be classified and marked as Confidential Privileged Information (CPI). (Sample CPI marking included at "Attachment A") Any persons on the

developer's planning and design team who will be involved in generating or handling AUS CPI shall be required to execute a Non-Disclosure Agreement (NDA) with AUS.

No person shall apply the Security Sensitive Information (SSI) designation to any information/materials without the expressed consent of the Airport Security Manager or an authorized representative of the TSA. Once any information is marked as SSI, it may only be stored and disseminated under the terms of 49 CFR 1520.9.

5. Terminal Roadways and Exterior Areas

5.1 Terminal roadway approaches and exits [non-restricted area]

5.1.1. Vehicle inspection locations. Under Imminent Threat conditions of the National Terrorism Advisory System (NTAS) or when otherwise directed by TSA, AUS is required to conduct inspections of vehicles that will approach within 300 feet of terminals. Terminal approach roadways shall include adequate space for the placement of vehicle inspection locations. These placement shall allow for the placement of barricades (moveable or fixed) to provide a crash rated barrier separating AUS personnel from through lanes of traffic, variable message signage, and alternate routes to direct away operators of vehicles who arrive at the vehicle inspection location but decline to submit to inspections. Vehicle inspection locations should include adequate CCTV coverage (viewable from the AOC and vehicle inspection location) to observe approach to vehicle inspection location, AUS personnel and exterior of vehicles at inspection location (including under and above vehicle views), vehicle exit to alternate route and terminal approach from vehicle inspection location. Vehicle inspection locations shall include a fixed structure capable of sheltering (protection from cold, heat, rain, etc.) up to 3 personnel for 4 hour shifts or provide adequate space for staging of a portable/temporary structure to meet the same standards and portable utilities.

5.1.2. CCTV roadway placements. Fixed CCTV placements to support License Plate Reader (LPR) technology capable of capturing all vehicles entering the roadway(s) leading to terminals prior to parking lot entries should be placed. Additional fixed CCTV placements capable of tracking vehicle movements from point of entry onto terminal approach roadways to point of exit shall be placed.

5.1.3. Dedicated emergency vehicle access routes. A dedicated emergency vehicle ingress/egress route or lane shall be included for all terminal approach roadways. This route may also serve as AUS operations/maintenance route or improved roadway shoulder when not in use by emergency vehicles but shall include adequate measures to prevent general public use.

5.2 Terminal frontage roadways, curbsides, sidewalks, and pedestrian crossings [non-restricted area]

5.2.1. Ramming protection. Design shall incorporate vehicle ramming protection for persons on curbsides and the terminal to provide maximum standoff potential distances – in general, protection should be placed no greater than 4 feet from the roadway curb adjacent to the area being protected. Ramming protection shall be rated at ASTM C40 P1 rating (capable of stopping a 5000lb vehicle traveling at 30mph) or higher as appropriate for roadway speed and permissible vehicle types.

5.2.2. Sufficient lanes. Design shall provide a sufficient number of traffic and passenger drop-

off/pick-up lanes to minimize vehicle congregation/congestion.

5.2.3. Signage. Adequate markings and signage shall be provided for enforcement of no parking/no waiting measures. Adequate markings and signage shall be provided to indicate loading/unloading is not allowed in through traffic lanes.

5.2.4. Pedestrian crossings. Adequate measures shall be included to allow for safe pedestrian paths to access adjacent parking, ground transportation areas, and support facilities. Pedestrian paths shall utilize means to minimize management by AUS staff – such means may include elevated or below surface pedestrian pathways and automated crossing beacons. Approaches to pedestrian crossings shall be designed to deter "jaywalking" or crossing of roadways at points other than designated crossings – such measures may be incorporated with vehicle ramming protection to serve dual intent.

5.2.5. Baggage check/drop counters. Adequate queueing accommodations shall be included to prevent interference with pedestrian crossings, terminal entrances, and roadways. Physical queueing spaces and/or approved airline operator queue management plans may be used to satisfy this requirement.

5.2.6. Public announcement system. Adequate public announcement measures, incorporated into the Airport's PA system, shall be included in all terminal roadside areas for public announcements to remain clearly audible and understandable under the maximum expected vehicular ambient noise load.

5.2.7. CCTV placements. Fixed CCTV placements to support LPR technology of all vehicles arriving at terminal curbside shall be placed. Fixed CCTV placements shall be placed to allow view of the entirety of terminal roadways, curbsides, sidewalks, and pedestrian crossings; and, to minimize "blind spots" caused by vehicles and pedestrians. Additional pan, tilt, zoom (PTZ) CCTV placements shall be made to supplement fixed CCTV views of areas of high potential pedestrian traffic and/or congregation; such areas include bus stops or other dedicated mass ground transportation areas, pedestrian crossing paths, terminal entrances, curbside baggage check/drop counters, pet relief areas, and any other areas identified by AUS.

5.2.8. Bicycle storage locations. Public bicycle storage locations should not be allowed within 300 feet of terminal structures. Any public placements within 300 feet of terminal structures must provide blast separation (such as described in 5.3.1 of this guide) from terminal interiors and curbsides. All bicycle storage locations within 300 feet of terminal structures must be removed under Imminent Threat conditions of the National Terrorism Advisory System (NTAS) or if a specific threat is identified by AUS Airport Security.

Employee bicycle storage locations within 300 feet of terminal interiors and curbsides may only be placed in areas outside of public view, under CCTV coverage, and with adequate protection to minimize blast effects; such placements shall also include measures to prevent public use, such as: prohibitory signage and physical barriers.

5.2.9. Public lockers are not permitted in any portion of terminal buildings or any adjacent areas within 300 feet of terminal buildings. Any structures that may serve as impromptu lockers must receive Airport Security approval when placed within 300 feet of terminal buildings regardless of intended use- such items may include: mail boxes, drop boxes, and equipment cabinets.

5.3 Terminal entrances, curtain wall, and façade glazing system [non-restricted area/restricted area barrier]

5.3.1. Blast protection walls. Exterior terminal walls shall incorporate a blast debris mitigating system that shall provide a level of protection equal to or greater than that identified under the latest AUS Blast Analysis. Exterior walls shall provide a "high level" of protection and "low hazard level" as defined by the ISC Security Design Criteria for Federal Buildings, consistent with GSA Performance Condition 3b or better, when forming a boundary of

FIS/CBP, TSA, loading docks/service entries, curbside baggage check/drop areas, or passenger screening areas.

5.3.2. Exterior glazing panels. Exterior glazing panels shall meet ASTM F2912-17 Standard Specification for Glazing Systems Subject to Air Blast Loadings.

5.3.3. Public terminal entrance/exit vestibules. Under Imminent Threat conditions of the National Terrorism Advisory System (NTAS) or when otherwise directed by TSA, AUS is required to limit terminal access in arrivals areas. Doors in these vestibules shall be capable to operate in both "entry and exit" and "exit only" modes.

5.4 Terminal loading docks and other service entries used for the introduction of merchandise/consumables and processing of materials/tools for terminal sterile areas. [non-restricted area/restricted area barrier/portal] AUS utilizes a remote Central Receiving and Distribution Center (CRDC) to perform mandated screening of merchandise and consumables sold/utilized within terminal sterile areas. All terminals are required to incorporate an adequate number of dedicated locations capable of receiving palletized transfer of goods from the CRDC to support concessionaire operations – such locations are referred to as terminal loading docks. When terminal loading docks serve as non-restricted area to restricted area portals, they shall also include adequate provisions to be utilized to conduct spot employee/item screening by AUS/TSA personnel and for the processing of contractor materials and tools for terminal construction activities. The following design and operation criteria shall be included:

5.4.1. Perimeter barrier with vehicle and pedestrian access gates. A perimeter barrier controlling vehicular and pedestrian approach to loading dock areas from public areas of the Airport's shall be included, and shall be of sufficient design to reasonably prevent public entry. Vehicle and pedestrian access gates to the loading dock approach area shall be incorporated into the Airport's automated access control system and capable of supporting "badge and code" and "code" only operation.

5.4.2. CRDC parking and contractor vehicle inspection area. Adequate parking locations shall be included within the loading dock perimeter fencing to support CRDC and other supported operations, such as; trash and grease removal services, maintenance support services, construction dumpster staging, and security agent parking. Adequate space shall also be provided for contractor offloading of materials and tools.

5.4.3. Sally port corridor. A "sally port" corridor for transfer of palletized goods from terminal exterior into terminal service corridors or concession storage spaces shall be incorporated into the Airport's automated access control systems capable of forming an "interlock" preventing both ends of the corridor from being open at the same time.

5.4.4. Pedestrian door. A pedestrian "bypass" door from terminal exterior into terminal service corridors or concession storage spaces shall be included and integrated into the Airport's automated access control system.

5.4.5. External "call-box"/telephone. A "call-box" or telephone shall be provided in close proximity to exterior of sally port/pedestrian door so that contractors may contact the Security Agent Office or Airport Operations Center when the Security Agent Office is not staffed.

5.4.6. Security Agent Office. A climate controlled office providing either open view or CCTV view of loading dock vehicular areas, sally port area, and pedestrian door(s) shall be incorporated into loading dock areas. The office shall be of sufficient size to provide workspace for 1 person; including: an automated access control workstation; an Aviation domain computer workstation with printer/scanner/copier; landline telephone; and, adequate electrical outlets to support radio charging stations or other office devices.

5.4.7. CCTV placements. Fixed CCTV placements to support LPR technology of all vehicles entering loading dock perimeter barriers. Fixed CCTV placements shall be placed to allow view of the

entirety of loading dock vehicular areas, access portals, inspection areas, and adjacent terminal service corridors and concessionaire storage areas. CCTV placements shall be adequate to minimize "blind spots" caused by pedestrians, vehicles, or goods.

5.5 Terminal rooftops. [restricted area] Consideration must be given to avoid unauthorized access to terminal rooftops. All exterior walls shall provide equal or greater climb protection than adjacent secured area fencing. Public stairwells and elevators shall not provide rooftop access. All portals providing rooftop access shall be incorporated into the Airport's automated access control system to provide "badge in/badge out" capabilities. CCTV placements covering terminal rooftops may be limited to fixed CCTV monitoring of ACS portals and any other AUS identified areas of concern.

6. Security Design Considerations for Terminal Interior Areas

6.1 General Considerations

6.1.1 Public lockers are not permitted in any portion of terminal buildings or any adjacent areas within 300 feet of terminal buildings.

6.1.2 Public accessible stairwells and elevators in terminal. Public accessible stairwells and elevators may not serve as non-restricted area to restricted area portals.

6.1.3 Non-restricted area to restricted area barrier walls, partitions, and portals. All barriers between the non-restricted area to restricted areas of the terminal shall be of adequate construction and full height (floor to ceiling - or having other adequate and AUS Security approved measures) to prevent persons or items from traversing the barrier – this includes being thrown across or passed under doors/gates. All portals (as described within section 4.5) shall be integrated into the Airport's automated access control system and configured to support "badge in/badge out" operations.

6.2 Non-Sterile to Sterile Area Portals in Public Areas. Portals directly accessing the sterile public areas of the terminal from public non-sterile areas shall be limited to: passenger screening checkpoints and associated "bypass" lanes for Known Crew Members (KCM) and emergency responders; employee screening checkpoints (further described in section 6.2.1.); staffed or automated sterile area passenger exits (further described in section 6.2.3.). All such portals must include ACS and CCTV support as deemed required by AUS and applicable TSA personnel. Employee access portals providing access from non-sterile to sterile areas other than those previously described must utilize a restricted area corridor configuration requiring employees to traverse through a restricted area; and, must be controlled through the automated access control system.

6.2.1. Employee/worker screening portal. Federal regulations require that Airport workers be subject to screening activities. If such workers submit to screening at TSA passenger screening checkpoints they are subject to passenger screening standards. This may result in workers not being able to bring in certain items/tools necessary for their duties. To account for this, airports may establish and operate separate worker screening portals in which such items/tools may be admitted.

6.2.1.1 Co-located worker screening portal. AUS recognizes the most efficient means to conduct worker screening operations is a hybrid model in which TSA conducts personnel screening activities and AUS screening be limited to worker items/tools. To facilitate this model a separate but immediately adjacent item screening corridor (leading from public checkpoint approach to sterile side passenger reassembly area) should be located in conjunction with passenger screening checkpoints to provide for screening of worker items. The corridor shall provide visibility to the passenger screening checkpoint but maintain physical separation. The corridor shall be of

sufficient size to house explosive trace detection and/or carry-on bag size x-ray screening technologies and require minimum staff effort to move screened items through. The corridor shall have access control doors on either side to allow for positive closure of the corridor if not staffed. CCTV placements of the corridor shall be consistent with those of the passenger screening checkpoint.

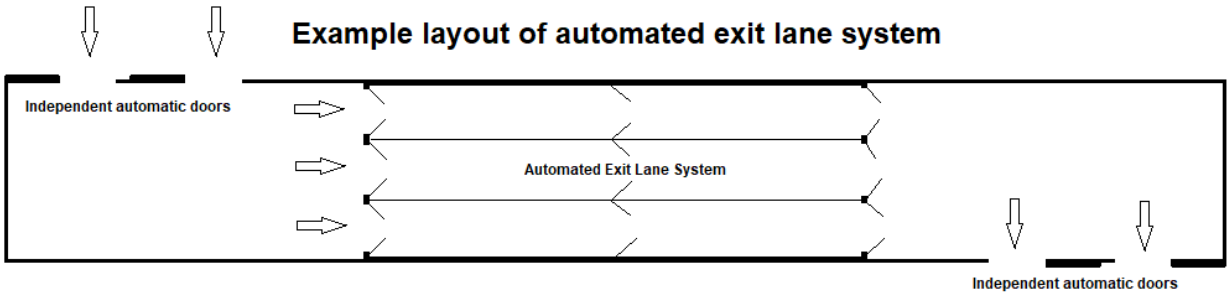
6.2.1.2 Independent worker screening portal. If a worker screening portal is not located in conjunction with a passenger screening checkpoint, it most include accommodations for both personnel and item screening. It would be the intent of AUS that TSA operate such a portal, as such, the design should mimic that of a TSA passenger screening checkpoint as described in section 6.4 of this guide.

6.2.2. Passenger sterile area exits must include measures to prevent unauthorized entry/backflow into the sterile area. Passenger sterile area exits should be placed out of direct view of passengers in non-restricted areas of the terminal, so as to deter identification as a potential sterile area entry route.

Examples of sterile area exit angled from normal direction of travel to deter accidental entry:

Sterile side entry into exits shall visually cue passengers that they are transitioning out of the sterile area. Each side of the exit shall include floor, eye level, and elevated signage to clearly indicate the direction of travel and that re-entry into the sterile area is prohibited.

Positioning and type of automated exit lanes must be approved by the AUS Security Manager (who will facilitate TSA review). Automated exit systems shall be integrated into the ACS to allow for lockdown of the system, lock-open of the system, wrong-way alarm activation, left object alarm activation, “prop” open alarm activation, and forced open alarm activation. Automated exit system placement shall include an independent automatic doorway on the non-restricted side of the system with pedestrian sensors only initiating door operation from the sterile side facing of the door. Automated exits shall include an independent automatic doorway on the sterile side of the system with pedestrian sensor only initiating door operation form the sterile side of the door that shall be placed no closer than 15 feet to the automated exit system entry – further placement restrictions may be imposed on a case-by-case basis dependent on system configuration and placement. The independent sterile side automatic doorway shall be integrated into the ACS so that the door closes and the pedestrian sensor deactivates upon command from the ACS. Door widths of independent automatic doorways shall be designed to accommodate single pedestrian access to ADA specifications, and cycle times shall be sufficiently short to deter backflow from pedestrians traveling in the wrong direction.



Passenger exit lanes shall have adequate CCTV coverage to cover the entirety of the exit lane area while minimizing "blind spots" resulting from pedestrian users. CCTV placements shall be sufficient to track the movement of persons entering and exiting the areas until under the coverage of existing/other CCTV placements.

6.3 Terminal Non-Sterile Public Areas. [non-restricted area/restricted area barrier] Terminal non-Sterile Area public areas consist of all areas accessible to the non-traveling public and adjacent areas not separated by automated or manual access controls and signage. Non-sterile public areas of the terminal include: airline ticketing counters/offices (unless separated by automated access control portals); baggage claim and associated airline baggage offices; 'pre-security' retail stores/restaurants, elevators, escalators, and restrooms. [Areas of the terminal accessible to the traveling public by entry through passenger screening checkpoints are classified as sterile areas and covered in section 6.4.]

6.3.1 Emergency threat mitigation. Due to their vulnerability to a wide variety of threats, consideration to mitigate these threats must be incorporated into the design of airport terminals. The following are general considerations that must be included in design of terminal public areas: maximize the ballistic and blast protection offered by millwork, columns, and building structural features; balconies, stair landings, and other publically accessible locations shall have partitions of sufficient height (6 feet or greater) to prevent use as a "perch"; controlled access observation posts with ballistic protection should be included for AUS law enforcement and security personnel; areas shall be planned to provide easy egress in the event of emergency while also offering the greatest "sheltering in place" potential; and, current threat mitigation technologies shall be evaluated and incorporated into design as deemed required by AUS Security, Operations, Information Systems, or Planning and Development personnel.

6.3.2 CCTV placements. Fixed CCTV placements shall be placed to allow view of the entirety of terminal public areas, excluding interiors of restrooms and enclosed office spaces under the sole lease holding of one tenant. CCTV placements shall be adequate to minimize "blind spots" caused by pedestrians and furnishings/millwork. Dedicated fixed CCTV placements shall support each automated access control portals, to include inline baggage screening belt access points. Additional pan, tilt, zoom (PTZ) CCTV placements shall be made to supplement fixed CCTV views of areas of high potential pedestrian congregation such as entry/exit vestibules, main walkways, screening checkpoint entries and supplemental queuing areas, baggage carousels, and sterile area exits.

6.3.3 Public announcement system. Adequate public announcement measures, incorporated into the Airport's PA system, shall be included in all terminal areas for public announcements to remain clearly audible and understandable under the maximum expected ambient noise load.

6.3.4 Ticket counter queuing areas. Adequate queueing accommodations shall be included to prevent interference with pedestrian paths, adjacent counter entrances/exits, and passenger screening operations. Physical queueing spaces and/or approved airline operator queue management plans may be used to satisfy this requirement.

6.3.5 Baggage claim devices. So as to deter baggage theft and introduction of unscreened baggage/items, baggage claim devices shall include perimeter railings or other means to prevent

direct entry and intermingling from the general public area. Entries and exits to devices shall include enhanced CCTV placements capable of supporting "left item" detection.

6.4 Terminal Sterile Public Areas. Terminal sterile public areas are those areas of the terminal accessible to the traveling public through the passenger screening process. Sterile public areas of the terminal include: airline gate holding/seating areas; 'post-security' retail stores/restaurants, elevators, escalators, and restrooms; and, walkways connecting the afore mentioned areas.

6.4.1 CCTV placements. Fixed CCTV placements shall be placed to allow view of the entirety of terminal public areas, excluding interiors of restrooms and enclosed office spaces under the sole lease holding of one tenant; such as an airline club. CCTV placements shall be adequate to minimize "blind spots" caused by pedestrians and furnishings/millwork. Dedicated fixed CCTV placements shall support each automated access control portal. Additional pan, tilt, zoom (PTZ) CCTV placements shall be made to supplement fixed CCTV views of areas of high potential pedestrian congregation such as entry/exit vestibules, main walkways, screening checkpoint exits, and entries into sterile area passenger exits.

6.4.2. Sterile Area to Secured Area Portals. Direct sterile area to secured area portals are required to be limited to the minimum required for operational support. Consideration shall be made to have such portals outside of public view. Safety considerations shall be made if portals are to serve as public fire and/or emergency exits to account for public exiting into the active aircraft operations secured area. All such portals capable of being "forced open" shall have delayed egress devices integrated into the Airport's ACS and fire detection systems as covered by the latest AUS/Austin Fire Department MOU (provided on a need to know basis by AUS). All portals shall be integrated into the Airport's ACS configurable for "badge in/badge out" operation, this includes jet bridge doors leading from gate holding areas into the jet bridge and jet bridge doors providing pedestrian exit to the Secured Area.

6.4.3. Public announcement system. Adequate public announcement measures, incorporated into the Airport's PA system, shall be included in all terminal areas for public announcements to remain clearly audible and understandable under the maximum expected ambient noise load.

6.4.3. Airline holding gate queuing areas. Adequate queueing accommodations shall be included to prevent interference with pedestrian paths, adjacent counter entrances/exits, and passenger screening operations. Physical queueing spaces and/or approved airline operator queue management plans may be used to satisfy this requirement.

6.4.4. Gates/doors on stores/restaurants required. All tenant stores and restaurants must include a means to physically secure any consumables/merchandise stored and/or displayed within the venues at any time the venue is not in operation. If grated security gates are used, consumables/merchandise shall be stored far enough away from gates or openings in the gates shall be small enough to prevent persons from reaching through the gates to access consumables/merchandise. Manual vending or display kiosks (meaning public has free access to consumables/merchandise displayed) located outside of stores/restaurants must include a means to be removed or locked when staff is not present to monitor.

6.5 TSA Passenger Screening Checkpoints. While in operation, TSA passenger screening checkpoints are operated by and under the control of local TSA personnel. When not in operation security of the passenger screening checkpoints and related portals are maintained by the AUS ACS and CCTV systems. In addition to meeting standards within the most current version of the TSA Checkpoint Design Guide, any project affecting TSA passenger screening checkpoints requires coordination with both AUS Airport Security and local TSA representatives.

6.5.1. TSA Coordination. For projects affecting passenger screening checkpoints, AUS shall either serve as the TSA point of contact (POC) for tenants/contractors or provide a direct TSA POC dependent upon project extent. TSA shall determine/approve configuration of passenger

screening areas.

6.5.2 Checkpoint perimeter/barrier. Both TSA and AUS Airport Security shall be consulted regarding required considerations for securing the checkpoint area both when in and not in operation. Barriers separating the TSA passenger screening checkpoint from non-restricted areas shall be sufficient to prevent the introduction of unauthorized persons or items when not in operation; such measures shall include a full height (floor to ceiling) barrier. A barrier shall also be included to deter/prevent unauthorized persons within the Sterile Area from entering the TSA passenger screening area when not in operation.

6.4.3 Law Enforcement Officer (LEO) station/podium. Under the terms of 49 CFR 1542.215 and the Geraldo Hernandez Airport Security Act, airport operators must station at least one LEO per TSA passenger screening checkpoint with additional LEOs as required to maintain a 6 lane to 1 LEO ratio per checkpoint. An elevated LEO station/podium offering ballistic protection (equal or greater tan NIJ type IIIA) to the passenger screening area and visible adjacent public areas shall be included to provide the best practical view of the associated 6 passenger screening lanes and public approach. Stations/podiums shall be adequate to provide physical contact shielding of LEOs on remaining sides not containing ballistic protection. Stations/podiums shall have adequate data and electrical outlets to each support one officer and related equipment (radio/phone chargers).

6.5.4 ACS placements. In addition to access portals, additional placements to allow for verification of AUS issued access/identification media at TDS podiums and covert ACS placements for "panic buttons" shall be included as deemed by TSA, APD, and AUS Airport Security.

6.5.5 CCTV placements. In addition to sufficient fixed placements to support viewing of the entire screening and queuing areas to minimize occlusions caused by persons, equipment, and millwork, additional placements to cover 'hotspots' as identified by TSA and AUS Airport Security shall be included.

6.6 Terminal Sterile Non-Public Areas

6.6.1 Non-SIDA/Sterile areas – These areas consist of terminal sterile areas not intended for public use. Such areas may include but are not limited to: housekeeping/plumbing closets, storage rooms, and concessionaire kitchens. Such areas not intended for public access but not separated by ACS portals must include a means to ensure they are kept secure. If not integrated into the AUS ACS, access to spaces must be controlled through doors with automatic closing devices (electric, pneumatic, hydraulic, spring); and, door hardware must not be capable of being set to allow free entry from publically accessible areas. Any potential access portals other than doors, such as restaurant kitchen to counter windows, must include a means to physically secure the portal when not in use.

6.7 Terminal areas used for storage of sterile areas goods (merchandise/consumables). Inspected merchandise and consumables delivered to the terminal from the CRDC must be kept separate from uninspected goods in an approved secured and monitored location until introduced into the sterile area. Merchandise must also remain in approved storage locations and utilize approved routes. AUS CCTV placements must be capable of monitoring goods from the point of delivery to placement within storage areas and from removal of storage areas until introduction into the sterile area. Spaces used to store or stage such goods with access portals not integrated into the AUS ACS are limited to spaces within terminal Sterile Areas and must have doors/gates with automatic closing devices (electric, pneumatic, hydraulic, spring); and, door hardware must not be capable of being set to allow free entry from areas accessible to persons not associated with the storage/delivery of goods.

7. Security Design Considerations for Airfield Security Identification Display Areas (Secured Areas, Air Operations Areas, and other Security Identification Display Areas) [Restricted Areas]

7.1 Fencing standards. Fencing serving as non-restricted to restricted area boundaries or traversing separate areas defined under 49 CFR 1540.5 shall be constructed of an AUS approved "non-climbable" material and topped with coiled concertina wire – details available in AUS fencing standard, provided on an as needed basis.

7.2 Clear zones – AUS clear zones consist of a 5 foot area on each side of AOA and Secured Area fence. Within clear zones that shall be no stored materials, no parked vehicles/equipment, trees, utility poles, or visual obstructions not individually approved by AUS Airport Security. When items (such as gate drive units, protective bollards, intersecting non-AOA and Secured Area fence lines) are approved to be within the clear zone by AUS Airport Security, additional security mitigations may be imposed on a case-by-case basis.

7.2.1. Ramming protection for Secured Area and Air Operations Area fencing – When serving as the non-restricted to restricted barrier, secured area and air operations areas, fencing along roadways and other areas to which vehicles have access, shall incorporate a continuous crash resistant barrier - unless other structures and/or geographical features are identified by AUS as serving as an acceptable barrier. Crash resistant barriers shall either form or be outside of the exterior clear zone boundary of fence lines. AUS Property Management and Business Development and/or AUS Planning and Development may impose further requirements for crash resistant barriers, including aesthetic considerations.

7.2.2. CCTV and Perimeter Intrusion Detection Systems – CCTV placements shall be sufficient to allow for monitoring of fence lines serving as non-restricted to restricted area barriers; including, entirety of interior clear zones in support of video analytic Perimeter Intrusion Detection Systems (system information will be provided by AUS on a need to know basis).

7.2.3. Marking and signage – Adequate signage and markings shall be provided so that clear zone requirements are readily observable. Interior clear zones within areas in which ground service equipment is operated or stored, ground markings shall be included to indicate boundaries – where possible, these markings shall be supplemented by AUS Operations approved low or standard height traffic barriers.

7.3 Gates

7.3.1. Direct public non-restricted area to Secured Area access gates. Federal regulations require that identity verifications and inspections of vehicles/property be conducted at direct Secured Area entry points from non-restricted areas and any addition/change of such an entry point requires direct AUS Airport Security Manager approval. To facilitate required inspections the following shall be included:

7.3.1.1 Speed limiting devices. Adequate measures to reasonably limit exterior gate approach speeds to 15mph or less. Speed limiting signage shall be included but is not sufficient to serve as the sole means (potential measures include speed "humps" and serpentine barriers, but shall be evaluated and approved on a location specific basis).

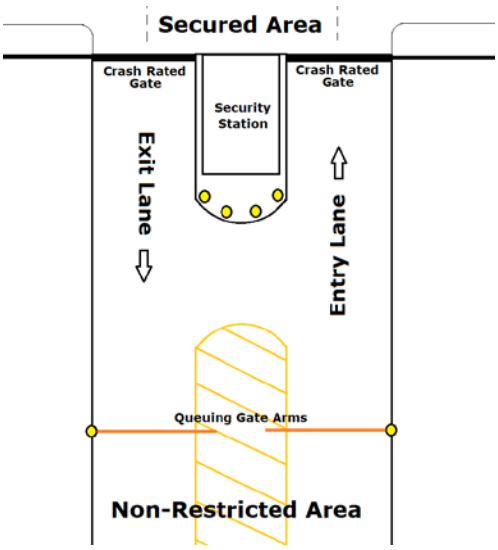
7.3.1.2 Personnel and vehicle inspection signage. AUS Airport Security approved signage shall be included to notify approaching personnel of inspection and security requirements of location – signage wording and size requirements will be provided by AUS Airport Security.

7.3.1.3. Vehicle queueing lanes. Exterior gate approach shall provide adequate space to ensure vehicles queued awaiting access to not block or pose traffic hazards on adjacent roadways.

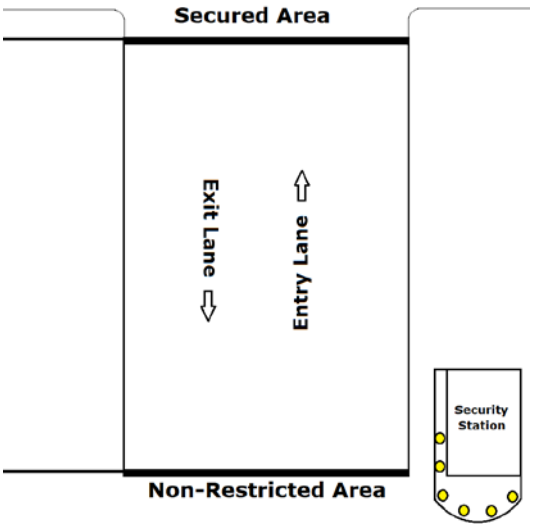
7.3.1.4. Vehicle gate configurations.

- Two single lane (one for entry and one for exit) crash rated security gates shall be utilized at each vehicle entry point – in addition to a shorter "open" time and reduced cycle count from a single dual lane gate, this allows for continued contingency use of the entry point as a single lane two-way traffic gate should either gate fail. An additional gate or gate arm shall be included on the exterior of both the crash rated entry and exit gate to provide a vehicle inspection station prior to entry through crash related gates. Series of operations shall be specified by AUS Airport Security.
- Sally port configuration. If spatial restrictions prohibit the two lane configuration, AUS will consider alternate means providing like security and contingency measures. One such example would be a sally port configuration.

Dual lane gate layout



Sally port gate layout



7.3.1.5 CCTV Placements. Primary vehicle inspection area should include adequate CCTV coverage (viewable from the AOC and vehicle inspection location) to observe approach to vehicle inspection location, AUS personnel conducting inspection, and exterior of vehicles at inspection location (including under and above vehicle views). Fixed views shall also be provided of all exterior ACS controls, gates, and adjacent fencing.

7.3.1.6 ACS Placements. ACS placements and series of operations shall be specified AUS Airport Security. ACS placements will provide the ability to conduct verification of access/identification media independent of gate operation, support badge in/ badge out operation of each gate, and be capable of remote operation and lockdown from AOC. Gates shall generate a "forced open" notification within the ACS if opened greater than 5" without use of the ACS. Gates shall generate a "hold open" notification within the ACS if it fails to completely close (greater

than 4" opening) within an AUS programmable time after being activated through the ACS.

7.3.1.7 Gate activation beacon. Gates shall include a prominently placed and visible beacon that shall flash to indicate when the gate is cycling either open or closed. The beacon shall cease to flash when the gate has returned to fully closed/secured status.

7.3.1.8 Security Station. Security inspection location shall include a fixed structure capable of sheltering (protection from cold, heat, rain, etc.) up to 3 personnel for 4 hour shifts. The station shall be of sufficient size to provide workspace for an automated access control workstation; an Aviation domain computer workstation with printer/scanner/copier; landline telephone; and, adequate electrical outlets to support radio charging stations or other office devices.

7.3.1.9 External "call-box"/telephone. A "call-box" or telephone shall be provided in close proximity to exterior of the security station so that stakeholders may contact the Airport Operations Center to perform escort notifications or request additional assistance.

7.3.1.10 Pedestrian use of vehicle gates prohibited. AUS security regulations prohibit the use of vehicle gates by pedestrians. If pedestrian entry is required, a separate ACS pedestrian gate or turn-style must be installed – each such placement requires direct approval of the Airport Security Manager. Design requirements of pedestrian direct secured entry gates will be reviewed and approved on a case by case basis.

7.3.1.11. Security of gate control boxes. Motor control boxes or other devices capable of allowing gate operation outside of ACS activation shall include an approved means to prevent/detect unauthorized access.

7.3.2 Non-AOA SIDA to Secured Area access gates. TSA Regulatory personnel classify such gates as public to Secured Area access gates; and, therefore, require that identity verifications and inspections of vehicles/property be conducted as at direct Secured Area entry points from non-restricted areas and any addition/change of such an entry point requires direct AUS Airport Security Manager approval. To facilitate required inspections all of the measures associated with direct public non-restricted area to Secured Area access gates described in section 7.4.1. of this guide are applicable with the exception that vehicle gates need not be crash rated.

7.3.3 AOA access gates adjacent to Secured Areas. As stated in CFR 1540.5, Secured Areas also include adjacent areas not separated by adequate security measures. Gates providing AOA access from non-restricted areas or non-AOA SIDAs that are not separated by adequate security measures from Secured Areas are subject to being considered Secured Area gates; and, are subject to all requirements as listed in section 7.3.1. or 7.3.2. of this guide. The AUS Airport Security Manager shall make any determinations of what constitutes adequate security measures for purposes of Secured Area separation. Potential examples of acceptable separation include: requirement to traverse through an active aircraft movement area (taxiway/runway); distance separation greater than 1/4 mile; and/or separation through natural or manmade barriers.

7.3.4 Non-AOA SIDA and AOA access gates not adjacent to Secured Areas. Gates providing access from non-restricted areas to any SIDA other than a Secured Area, do not require constant stationing of personnel to conduct vehicle inspections. All requirements of described in section 7.3.1. of these guidelines are applicable to such gates with the following exceptions:

- Queuing gate arms as described in section 7.3.1.4. are not required;

- CCTV placements need only show exterior ACS controls, gates, and adjacent fencing; and
- Security station as described in section 7.3.1.8. is not required.

8. Security Design Consideration for Facilities with Direct AOA Access.

Facilities and structures serving as non-restricted area to restricted AOA boundaries must provide for adequate access control to prevent unauthorized entry into the AUS AOA. No structures other than terminals and fencing may serve as direct non-restricted area to restricted Secured Area boundaries.

8.1. Cargo Operations Areas. The following considerations are required for tenant cargo operator facilities forming a boundary between restricted/non-restricted areas:

8.1.1 Separation from passenger and general aviation operations. "All cargo" operations must have adequate separation from Secured Areas in which commercial passenger operations and general aviation operation areas.

8.1.2 Access control.

8.1.2.1 Automated access control systems. Cargo facilities must include access control portals capable of excluding the cargo facility from the AOA – all pedestrian and bay doors opening onto the cargo ramp must be under the control of the AUS automated access control system. Number and type of AOA access shall be consistent with federal regulations limiting the number to the minimum required to support operations – AUS Security and Tenant Management personnel may make determinations in this respect. Multiple bay doors may share a single access control reader – in this configuration, the card reader may be used to trigger a timed or circuit allowing activation of multiple door controls. All AOA access doors must generate a "forced open" alarm with the AUS ACS if opened without use of the card readers. Each AOA access door must prominently display the signage shown below or alternate signage approved by an AUS Airport Security Coordinator. Use of the AUS automated access control system to monitor/control the use of other facility doors may be required if necessary to control access to critical AUS infrastructure. Optional use of the access control system for additional facility doors may be approved on a case-by-case basis by AUS.

8.1.2.2 Non-AOA facility doors providing SIDA access. To conduct cargo screening operations within facilities, cargo operators must designate a portion of the facility as a SIDA. Operators shall clearly mark this area with either a physical barrier and/or ground markings. A drawing designating this area must also be submitted as part of the Airport Tenant Security Plan.

8.1.3 Blast analysis protection for cargo inspections areas. Cargo operators conducting TSA required cargo screening within their facilities shall establish a dedicated area for such inspections – this area shall be constructed to minimize the required evacuation areas should a suspect item be revealed. This area shall have a blast analysis conducted by a competent and experienced engineering firm with demonstrable like experience to determine recommended evacuation zones for the average size and type of items likely to be inspected within the facility. This study shall be provided to AUS Security and Project Management personnel.

8.1.4 CCTV coverage. AUS integrated CCTV coverage of cargo tenant facilities shall include: exterior doors/entryways both on public and restricted sides.

8.2. **Aircraft operator hangar and maintenance facilities.** Such facilities must meet the criteria as described for cargo operations areas under section 8.1 with the exception of section 8.1.3.

8.3. In-flight catering facilities. Such facilities must meet the criteria as described for cargo operations areas and must include the means that will be utilized to prevent tampering while transporting inspected deliveries to the Secured Area within their submitted Airport Tenant Security Plan.

8.4. Central Receiving and Distribution Centers. The Central Receiving and Distribution Center serves as the remote inspection center for all merchandise and consumables to be utilized with AUS Sterile Areas. The security requirements for the CRDC are included in the AUS Airport Security Program and will be provided on a as needed basis by AUS Security.

8.5. Fuel Farms. Size and location play a significant role regarding security considerations for Fuel Farms. As a minimum measure, Fuel Farms should have the same perimeter intrusion protection as exists for the AUS AOA. ACS and CCTV requirements will be decided by AUS Security on a case-by-case basis.

9. Security Design Considerations for General Aviation Areas.

As a minimum measure, General Aviation should have the same perimeter intrusion protection as exists for the AUS AOA though they will be excluded from the AOA through the use of a passive intrusion control system integrated into the AUS ACS and CCTV systems must be installed at all taxiway entryways into the AUS AOA from a General Aviation facility. Taxiway entries into the AOA may only be utilized by aircraft and entities with movement area driving authority (AUS operations/maintenance and emergency responders) – general aviation ground service vehicles may not utilize taxiways entries to access the AUS AOA. The remainder of the facility shall be separated from the AUS AOA as described in section 7.1-7.3 of this guide.

9.1. General Aviation vehicle access gates into the AOA shall follow the standards described under section 7.3.4 of this guide with the exception that a "call-box" as described 7.3.1.9 is not required nor may "spot" access requests for general aviation gates be routed by "call-box" or signage to the Airport Operation Center.

10. Security Design Considerations for Landside Areas.

10.1 General Considerations

10.1.1 CCTV placements. Fixed CCTV placements, incorporated into the AUS CCTV system) shall be included as deemed necessary by AUS Security to supplement any existing views affected by constructed landside facilities. Fixed CCTV placements shall be included of any common areas open to the general public with an expected increased liability risk - such areas include but are not limited: City of Austin, Arts in Public Places placements, playgrounds, and areas designed to facilitate public gathering.

10.1.2 Parking restricted within 300' of terminal structures. No landside facilities shall provide parking spaces within 300' of the terminal without written approval from the AUS Security Manager. All submitted requests for approval must include the methods used to provide blast protection equal to or greater than the 300' standoff; and, means used to prevent public parking within the area(s).

10.1.3 Clear zone and restricted area fence protection. All landside facilities adjacent to any AUS restricted area fence must include positive clear zone exclusion protection (such as parking stops in designated parking areas) and vehicle ramming protection (appropriate for use of facility) of the restricted area fence.

10.2 Aviation operated parking garages/parking lots shall have adequate lighting to provide for safe pedestrian transit of the area and discourage unlawful activities. CCTV coverage of lots should cover the majority of available parking areas and shall cover vehicle access/exit routes and areas of congregation (such as shuttle bus stops). Entrances shall include provisions for posting of airport operator required signage (such as federal face mask mandates).

10.3 Aviation Administration Support Building shall have CCTV views of all building entrances/exits and an overview of any reception desks and/or visitor staging areas. Entrances shall include provisions for posting of airport operator required signage (such as federal face mask mandates).

10.4 Tenant operated transportation facilities (public accessible/non-public accessible) shall have CCTV views of access pathways/routes. Adequate lighting to ensure safe pedestrian transit of areas and to deter unlawful activities shall be provided. Entrances shall include provisions for posting of airport operator required signage (such as federal face mask mandates).

10.5 Tenant operated facilities other. Entrances shall include provisions for posting of airport operator required signage (such as federal face mask mandates).

11. Project/contractor procedures for restricted area access.

Access to AUS restricted areas is limited to one of two means: 1) obtaining an AUS access/identification media; or, 2) being escorted by an authorized AUS access/identification media holder.

11.1 AUS access/identification media issuance process. To begin the process for issuance of AUS access/identification media (commonly referred to as an "Airport badge") a person must be sponsored by a company with an active operating permit with AUS. For most tenant projects, the tenant will be the sponsoring company; or, in the case of City of Austin/Department of Aviation projects an authorized AUS representative will serve as the sponsor. [More information regarding how to obtain an operating permit or how to conduct business at AUS is available under the "Business" tab of www.austintexas.gov/airport.]

11.1.1 Authorized Signatories. Each company capable of sponsoring AUS access/identification media must have one or more designated authorized signatories. These signatories serve as the subject matter experts for all contractor/project access/identification media issues; and, are the designated point of contacts between company/contractor access/identification media holders and the AUS Security and Identification Office. Authorized signatories are required to maintain current AUS access/identification media. (Sponsoring companies may be approved by the AUS Airport Security Coordinator - Badging to appoint a project/contractor employee with a current AUS access/identification to serve as a company authorized signatory.)

11.1.2 AUS Security and Identification Office. The AUS Security and Identification office processes applications for and issues AUS access/identification media under the terms of 49 CFR 1542.209. Communications to AUS Security and Identification Office regarding processes should be coordinated through company authorized signatories.

11.1.3 AUS access/identification media workflow for tenant projects.

a) Company authorized signatory completes application for contractor/project worker, verifying identity documents identifying means of payment for media and schedules appointment for worker with AUS

Security and Identification Office (sample application available at: www.austintexas.gov/sites/default/files/images/Airport/Internships_Employment/personal_information.pdf)

b) Worker reports in-person for appointment with Security and Identification Office - bringing completed application, the same identity documents listed on the application, and the form of approved payment indicated on the application.
c) Worker's biographical and biometric (fingerprints) information is collected by Security and Identification Office and submitted for background investigation (processing times average 1-2 weeks for those born within the US and 2-4 weeks for those born outside of the US).
d) AUS Security and Identification Office contacts company authorized signatory when background clearance is received or if results require worker to submit additional information.
e) Company authorized signatory coordinates with worker to schedule a second appointment with AUS Security and Identification Office to complete process or provide supplemental information.

11.1.4 AUS access/identification media workflow for City/AUS projects. Workflows for City/AUS sponsored projects are the same as described as for tenant projects in 11.1.3, except an AUS Project Manager will serve as the initial authorized signatory.

11.1.5 AUS access/identification media accountability. AUS issued access/identification media must be returned to AUS when the employee to whom the media was issued no longer requires access to AUS restricted area (either through termination, reassignment, or project completion).

11.1.6 Limitation on access. Airports are required to limit employees' access to the minimum required operational necessity. It shall be the responsibility of the authorized signer to indicate the paths and portals required for projects – this should be reflective of the requirement to limit access. AUS Security may deny any access requests deemed excessive or not consistent with the limitation requirements. Requests to add portals to employees' access media must be made through the company authorized signer – individual employees shall not contact the Security and ID office or other AUS Security personnel to request portal increases in AUS access media. Any emergent access needs shall be routed to the Airport Operations Center (512-530-2242), if deemed necessary, AUS personnel will be dispatched to grant momentary access.

11.1.7 Deactivation notice required. Company authorized signatories must notify AUS (through the Airport Operations Center at 512-530-2242) immediately if an employee no longer needs AUS access/identification media due to adverse an adverse separation/termination. In the event an employee no longer requires restricted area access due to routine reasons (completion of scope of work, voluntary transfer, etc.) notification to AUS must be made within 8 business hours.

11.1.7.1. Return of AUS access/identification media. After deactivation as described in section 11.1.5.1, AUS access/identification media must be returned to the AUS Security and Identification within 3 business days – it is the ultimate responsibility of the company authorized signatory . Failure to return access/identification media within these timelines will result in additional company fees and may also result in civil and criminal penalties. AUS access/identification media must also be

returned when: requested by an AUS representative; if the individual is no longer capable of possessing such media under the terms of 49 CFR 1542.209 (having been arrested or convicted of disqualifying offense after receiving the media); or, when no longer valid (such as expired).

11.1.7.2 Fees and penalties. AUS access/identification media not returned to AUS within timelines stated in 11.4.1 are subject to a "unreturned badge fee" of $100 per media – with the sponsoring company responsible for payment. Contractors sponsored directly by AUS are also subject to $500 per unreturned media being deducted from project payment. Misuse of access/identification may also result in civil and criminal penalties against individuals and sponsoring companies. Should AUS be issued a civil penalty due to a misuse of an access/identification media, the full penalty and additional costs of mitigation shall be paid by the individual or sponsoring company.

11.2. Escorted Restricted Area Access. For short-term restricted area access needs, AUS may allow the utilization of escorts (having the meaning assigned in 49 CFR 1540.5). Under an escort, an authorized AUS access/identification media holder (indicated by a supplemental marking on the media) shall constantly maintain responsibility for the movement and activities of a person or persons within an AUS restricted area who does not possess AUS access/identification media.

11.2.1 Obtaining escort authority. Company authorized signatories designate employees whom they wish to have escort authority during the processes described in section 11.1 or after access/identification media issuance through coordination with the AUS Security and Identification Office.

11.2.2 Escort responsibility. While conducting escorts, the authorized AUS access/identification media holder's primary responsibility shall be maintaining the terms of the escort. Any other duties performed by the authorized AUS access/identification media are secondary and should not conflict with his/her ability to constantly monitor and control the activities of those under escort.

11.2.3 Escort ratio. A standard escort ratio not exceeding 3 non-media holders to 1 authorized media holder shall be maintained unless an exception through an AUS Airport Security Coordinator is obtained – exceptions are limited to instances in which the ASC determines that work areas are far enough removed from other activities or allow for sufficient protections for ratios to be exceeded. The process for requesting escort ratio exceptions is provided by the AUS Security and Identification Office to authorized access/identification media holders at the time their escort authority is approved and the supplemental media marking is added.

11.2.4 Escort notification. Notification of all escorts must be made prior to the commencement of any escorts or change of personnel involved in any escorts. The process for escort notification is provided by the AUS Security and Identification Office to authorized access/identification media holders at the time their escort authority is approved and the supplemental media marking is added.

11.2.5 Escort limit. Persons requiring extended access to AUS restricted areas are required to under the processes described in 49 CFR 1542.209 for unescorted access. As such, attempting to escort a person 10 or more times within a 6 month period will cause an alert prompt when being communicated to the AOC or security representative. If a continued short term escort of individuals receiving this alert is needed, advance approval from an AUS Airport Security Coordinator is required.

11.3 Key access. Key access to project areas may occur through one of two methods: 1) contractor installs temporary locks in construction areas and provides for emergency access to AUS and emergency response personnel; or, keys to existing Airport installed locks are provided to contractors.

11.3.1 Contractor installed temporary locks. Contractor installed locks shall not interfere with operations of stakeholders not involved in the project. Contractor shall provide for emergency and routine access to AUS and emergency personnel through means agreed upon by AUS Project Management, Tenant Management, and Operations personnel

11.3.2 Airport provided key access. Project key access follows the same authorization chain as utilized for AUS access/identification media issuance described under section 11.1 of this guide. Requests for user keys shall be routed through company authorized signers utilizing the request forms provided to them.

11.3.2.1 Limitation on access. Airports are required to limit employees' access to the minimum required operational necessity. It shall be the responsibility of the authorized signer to indicate the paths and portals required for projects – this should be reflective of the requirement to limit access. AUS Security may deny any access requests deemed excessive or not consistent with the limitation requirements. Requests to add portals to employees' access media must be made through the company authorized signer – individual employees shall not contact the Security and ID office or other AUS Security personnel to request portal increases in AUS access media. Any emergent access needs shall be routed to the Airport Operations Center (512-530-2242), if deemed necessary, AUS personnel will be dispatched to grant momentary access.

11.3.2.2 Return of AUS access/identification media. After deactivation as described in section 11.1.5.1, AUS keys issued to contractors must be returned to the AUS Security and Identification office prior to project closeout. Failure to return keys within these timelines will result in additional company fees and may also result in civil and criminal penalties. A per item fee of $100 will be accessed for each key lost or not returned. Should loss/non-return of a key result in the requirement to replace locks to mitigate the risk resulting from the loss, the additional cost (including labor and materials) of the replacement shall be accessed to the project sponsoring company.

11.4 Vehicle access. Vehicle access to AUS restricted areas limited to those with a demonstrable need. Those vehicles meeting this requirement must meet one of the following requirements to be operated within SIDA areas: 1) Display a current and valid logo on file with AUS Security and be operated by an individual possessing current and valid AUS access/identification media appropriate for the SIDA in which the vehicle is being operated and having the appropriate driving privilege; or, 2) be continuously escorted by a person and individual meeting the requirements described in the previous option.

11.4.1 Vehicle logo registration. Vehicle logo registration follows the same authorization chain as utilized for AUS access/identification media issuance described under section 11.1 of this guide. The sponsoring company authorized signatory shall serve as the POC for contractors/subcontractors registering vehicle logos – individual employees should not contact AUS Security and ID or AUS Security regarding vehicle logo registration. Before submitting the logo application form (provided to authorized signers) to the AUS Security and Identification Office, the authorized signatory shall ensure the following conditions are met and indicated on the application:

- A certificate indicating minimum $5 million dollar vehicle liability insurance coverage has been submitted to the appropriate AUS Project Manager or Tenant Management representative, with a copy included with the application;
- Vehicle(s) display a highly contrasting logo on both the driver and passenger side of the vehicle – logo must have a minimum of 4" lettering and/or 12" logo and be clearly discernable from a distance of 200'. A color photograph or graphic image of the logo shall be included with the application. Logos of commercial equipment leasing/rental companies may not be registered unless the logo is clearly distinguishable from those available for public use.;
- At least one company employee of the logo being registered has a valid and appropriate AUS access/identification media and valid driver's license as described in City of Austin Municipal Code 13-1-133 – Driver's License Required:
- All vehicles to be operated within AUS SIDA must meet the vehicle safety requirements specified in City of Austin Municipal Code 13-1-138 – Vehicle Equipment Safety in Air Operations Area; and,
- Projected beginning and end dates of project must be listed.

The above should be submitted in an assembled packet to the AUS Security and ID office or may be emailed to: AUSCompliance@flyaustin.com

11.4.2 Vehicle escort. Vehicles only needing one time or limited access to an AUS SIDA may be escorted in lieu of submitting to the logo registration process. Conducting a vehicle escort requires that a vehicle with an AUS approved logo and operated by an AUS access/identification media holder with appropriate driving and escort authorities, continuously accompany a vehicle without an approved logo while within an AUS SIDA. If all occupants of the vehicle under escort possess AUS access/identification media, notification of the vehicle escort is not required. If an occupant of the vehicle under escort does not possess AUS access/identification media, the personnel escort requirements as described under section 11.2. of this guide must also be followed.

11.4.3 Restricted area driving authorization. Driving authorization/training is required for vehicle operation with the Secured Area and AOA, which are further divided into non-movement (ramp) or movement areas (runways/taxiways) for purposes of driver authorization and training.

11.4.3.1 Non-movement areas are those not under the control of FAA air/ground traffic controllers – this includes the terminal and cargo aprons and support service roads within the AOA. Authorization to operate a vehicle within these areas is indicated by the company authorized signatory during the AUS access/identification media process described under section 11.1. of this guide; if not indicated at that time, a company authorized signatory may request non-movement area driving authorization for an employee by submitting an updated AUS access/identification media application with the driving authorization indicated. Training for this authorization is conducted in conjunction with the AUS access/identification media on an annual basis. Non-movement area driving authorization is indicated by a sticker applied to the AUS access/identification media stating "Ramp Driving".

11.4.3.2 Movement areas are those areas under the control of FAA air/ground traffic controllers and the immediately adjacent safety zones. Movement area driving authorization is restricted to AUS Airport Operations, AUS Maintenance, and emergency responders as special equipment and training is required to operate on runways and taxiways. All other persons requesting access to AUS movement areas and/or movement area driving authorization should coordinate

through their Property or Tenant Management representative to coordinate with AUS Airport Operations.

11.5 Contractor tool check-in procedures/weapons prohibited. Only law enforcement officers and others specifically named in the AUS Airport Security Program are authorized to carry firearms with any AUS SIDA or where otherwise prohibited by local, state, and federal law. Only employees with an authorized and articulable need to possess any item deemed a "prohibited item" (listed as items prohibited from possession in carry on bags at: https://www.tsa.gov/travel/security-screening/whatcanibring/all) may possess such an item within any AUS SIDA or Sterile Area. Those possessing such items in an AUS Sterile Area must have logged the item in with AUS Security at the designated contractor check-in area (this is the main Loading Dock for the Barbara Jordan Terminal). Contractors may not be introduce such items into a Sterile Area through a TSA Passenger Screening Checkpoint or through an access control door. Once such items are inside the Sterile Area contractors must ensure that they are kept inaccessible to passengers. If such items are to remain inside the Sterile Area beyond a single work shift, they must be stored in a secured and locked job box or within a locked work area inaccessible to passengers. Contractors must conduct a daily inventory of all "prohibited items" remaining in the Sterile Area. Any unaccounted items must be immediately reported to the Airport Operations Center (512-530-2242). Contractors may receive badge revocation and civil penalties for incorrectly introducing an item into the Sterile Area or allowing a prohibited item to become publically accessible.

11.6 Terminal material delivery. Terminal material deliveries shall be directed to the contractor processing area (loading dock at the Barbara Jordan Terminal). Initial delivery shall be coordinated through the appropriate Tenant Manager or Project Manager. Once delivery schedules have been established, only large quantity or oversized deliveries will require additional coordination. Contractor terminal parking is not allowed. After unloading tools and/or materials at the contractor processing area contractors must move to a designated parking area.

11.7 Contractor parking arrangements. The designated AUS Tenant Management and/or Project Management will work with the contractor to identify appropriate parking arrangements for construction projects. Contractors deviating from agreed upon parking arrangements are subject to having their vehicles towed at their expense and receiving criminal and civil penalties.

11.8 Alternate access means – Security Guards. Alternate access is access into AUS restricted areas through any means other than those previously described in section 11 of this guide. Any alternate access must be approved by AUS Security; and, requests for alternate access requires a minimum of 45 days advance notice to allow for submission of amendments to the Airport Security Program. The most common used means of alternate access is through the temporary use of security guards to replace standard AUS access control systems during construction.

11.8.1 AUS provided security personnel. If deemed necessary due to previous violations or disablement of critical systems, AUS may require the use of AUS Security personnel to be assigned to a project (City of Austin Municipal Code, 13-1-54). If such is assigned, a minimum rate of 2X the midpoint salary of the personnel assigned shall be charged to project sponsoring company. An additional charge shall be assessed if an AUS vehicle is required to support operations. (Current rates will be provided by AUS Security Manager if assignment is required.)

11.8.2 Contractor provided security personnel. Use of contractor provided security personnel must be approved by the AUS Security Manager; and, all security personnel utilized in any AUS SIDA must submit to the AUS access/identification media process described in section 11. The roles of the security company may be limited as deemed appropriate by the AUS Security Manager. AUS does not authorize the use of armed security personnel in any AUS SIDA.

Attachment A – Confidential Privileged Information Marking Sample

[Header]

Confidential Privileged Information

[Document Body]

[Footer]

"WARNING": The attached is confidential privileged information property of the Austin-Bergstrom International Airport (AUS). It contains information requiring protection against unauthorized disclosure. The information contained in the attached document cannot be released to the public or other personnel who do not have a valid need to know without prior written approval of an authorized AUS official. The attached document must be controlled, stored, handled, transmitted, distributed and disposed of as approved by and authorized AUS official.

At a minimum, the attached will be disseminated only on a need to know basis and, when unattended, will be stored in a locked cabinet or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.