Kinexis Security Programm

August 2010

Approved by

The Walt Disney Company

Transportation Security Administration

Mickey Mouse Airportt

AIRPORT SECURITY PROGRAM

April 2024

Mickey Mouse Airport	**Transportation Security Administrator**
Airport Manager	**Federal Security Director / Transportation Security Inspector**
Name:	Name:
Signature:	Signature:
Date:	Date:

REVISIONS, UPDATES, AND AMENDMENTSs

The following table illustrates any revisions, updates, or amendments that have taken place since the initial approvals.

Number	Description of change	Page Numbers	Date Submitted	Date Approved

PURPOSEeeee

This document is submitted as the Kinexis Security Program (ASP) for Mickey Mouse Airport (KMMW) in Disney Corner, Florida. This program identifies the roles and responsibilities of the Airport as regulated by 49 Code of Federal Regulations (49 CFR), Transportation Security Regulation Part 1542.101(a). This ASP outlines participation from air carriers, tenants, and local law enforcement. The measures contained in this ASP are implemented to provide for the safety and security of individuals and property operating in air transportation at its facility against an act of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary onto an aircraft.

This ASP is applicable to KMMW and its tenants and operators regularly serving operations of aircraft operators. KMMW will ensure that employees, and representatives conducting security procedures on its behalf, comply with the provisions contained in this program.

ABBREVIATIONSssss

49CFR	Title 49 Code of Federal Regulation
ACS	Access Control System
AEP	Airport Emergency Plan
AIB	Airport Identification Badge
AOA	Airport Operations Area
AOB	Airport Operations Building
AOSC	Aircraft Operator Security Coordinator
AOSSP	Air Operator Standard Security Program
AS	Authorized Signatory
ASC	Airport Security Coordinator
ASP	Airport Security Program
ATC	Air Traffic Control
ATCT	Air Traffic Control Tower
ATSA	Aviation Transportation Security Act
CBT	Computer Based Training
CCAS	Changed conditions affecting security
CCTV	Closed Circuit Camera Television
CFR	Code of Federal Regulations
CHRC	Criminal History Records Check
CPU	Central Processing Unit
CMS	Credential Management System
CUG	Consolidated User Guide
DRO	Designated Ramp Observer
EDS	Explosive Detection System
eSF	eSecure Flight

ETD	Explosive Trace Detection
ETP	Explosive Trace Portal
FAA	Federal Aviation Administration
FAM	Federal Air Marshal
FBI	Federal Bureau of Investigation
FBO	Fixed Base Operator
FFDO	Federal Flight Deck Officer
FPRD	Fingerprint Results Distribution
FSD	Federal Security Director
GSC	Ground Security Coordinator
HHMD	Hand-held Metal Detector or “hand-wand”
IC	Information Circular
ICS	Incident Command System
ID	Identification Media Card / Badge
IdHS	Identity History Summary
IED	Improvised Explosive Device (VB=Vehicle Borne)
IMP	Incident Management Plan / Program
ISC	In-flight Security Coordinator
IT	Information Technology System
JTTF	Joint Terrorism Task Force
K9	Explosive Detection Dog Operations
LEO	Law Enforcement Officer
MNC	Manual name Check
MSP	Model Security Program (International Carriers)
NGI	Next Generation Identification
NIMS	National Incident Management System

NTAS	National Terrorism Advisory System
OPAC	On-Line Payment and Collection
ORI	Originating Agency Identification Number
PCSSP	Private Charter Standard Security Program
PIC	Pilot-In-Command
PID	Positive Identification
PSC	Passenger Screening Checkpoint
PTI	Positive Target Identification
RBN	Rap Back Activity Notification
RBUG	Rap Back User Guide
EFGH	Security Directive
SIDA	Security Identification Display Area
SOC	Standard Occupational Classification
SSI	Sensitive Security Information
STA	Security Threat Assessment
TA	Trusted Agent
TSA	Transportation Security Administration
TSC	Transportation Security Clearinghouse
TSO	Transportation Security Officer
TSR	Transportation Security Administration Regulations
KMMW	Mickey Mouse Airport
UID	Unique Identification
VBIED	Vehicle Borne Improvised Explosive Device
VID	Verifying Identity Document
WTMD	Walk-through Metal Detector

DEFINITIONSsss

Airport Categories: Airports governed by Title 49 of the Code of Federal Regulations (CFR) § 1542.103(a) are further defined as follows:

1. Category X: An airport regularly serving operations of an aircraft operator or foreign air carrier pursuant to 49 CFR § 1544.101(a)(1) or 49 CFR § 1546.101(a) and the number of annual enplanements is 5 million or more and international enplanements of 1 million or more.
2. Category I: An airport regularly serving operations of an aircraft operator or foreign air carrier pursuant to 49 CFR § 1544.101(a)(1) or 49 CF 1546.101(a)and the number of annual enplanements is 1.25 million or more.
3. Category II: An airport regularly serving operations of an aircraft operator or foreign air carrier pursuant to 49 CFR § 1544.101(a)(1) or 49 CFR 1546.101(a) and the number of annual enplanements is 250,000 or more, but less than 1.25 million.
4. Category III: An airport regularly serving operations of an aircraft operator or foreign air carrier pursuant to 49 CFR § 1544.101(a)(1) or 49 CFR § 1546.101(a) and the number of annual enplanements is less than 250,000.

Airports governed by 49 CFR § 1542.103(b) and (c) are further defined as follows:

1. Category IV: An airport regularly serving operations of an aircraft operator or foreign air carrier pursuant to 49 CFR §§ 1544.101(a)(2) or 1544.101(b) or 49 CFR §§ 1546.101(c) or 1546.101(d).

Air Operations Area (AOA): Means a portion of an airport, specified in the airport security program, in which security measures specified in this part, are carried out. This area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas for use by aircraft regulated under 49CFR Part 1544 or 1546, and any adjacent areas (such as general aviation) that are not separated by adequate security systems, measures, or procedures. This area does not include the Secured Area.

Aircraft Operator: Means a person who uses, causes to be used, or authorizes to be used an aircraft, with or without the right of legal control (as owner, lessee, or otherwise) for the purpose of air navigation including the piloting of aircraft, or on any of the surface of an airport.

Airport Operator: Means a person that operates an airport serving an aircraft operator or a foreign air carrier required to have a security program under 1544 or 1546

Airport / Airport Security Program: Means a security program approved by TSA under §1542.101

Airport Tenant: Means any person, other than an aircraft operator or foreign air carrier that has a security program under Part 1544 or 1546, that has an agreement with the airport operator to conduct business on airport property.

Airport Tenant Security Program: Means the agreement between the airport operator and the airport tenant that specifies the measures by which the tenant will perform security functions and approved by TSA under §1542.113.

Approved: Means approved by TSA, unless used with reference to another person.

Authorized Signatory: Any individual or designated representative authorized to sponsor individuals, collect, and transmit biographical data to the airport badging office, and request airport ID media for sponsored individuals.

Authorized Representative: For the purposes of this ASP amendment, an "authorized representative" is a person) for example, an air carrier, security contractor, concessionaire) who is authorized by the regulated party to carry out specific security functions for which the regulated party is responsible.

Attend: To assign specific personnel to be physically present in an area within the proximity of the delivery of merchandise and consumables to prevent unauthorized access. These personnel may be assigned additional duties as determined by the airport operator or authorized representative while simultaneously attending an area.

Biographic Data: Biographic Data is an individual's full name, date of birth, and gender. Redress numbers may be used in the resolution process.

Checked Baggage: Means property tendered by or on behalf of a passenger and accepted by an aircraft operator for transport, which is inaccessible to passengers during flight. Accompanied commercial courier consignments are not classified as checked baggage.

Consumables: For the purposes of this ASP amendment, a "consumable" is any food or drink, intended for sale to or sue by customers in the Sterile Area. It does not include company materials that need to be replenished, such as ticket stock, stationary products or similar materials intended for operation use

Criminal History Records Check (CHRC): A search for an individual's past criminal history by submitting a covered individual's fingerprints and biographic information to FBI's Next Generation Identification (NGI) and reviewing any criminal history records that FBI NGI returns.

Cybersecurity Incident: An event that, without lawful authority, jeopardizes, disrupts, or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the airport operator as a possible cybersecurity incident without final determination of the event's root casus or nature (such as malicious, suspicious, benign).

Escort: Maintain visual and voice control while monitoring the activities of an individual who does not have unescorted access authority into or within a Secured Area or SIDA

Fingerprint Distribution (FPRD): Secure online portal for airport operators to access fingerprint-based criminal history results received from the Federal Bureau of Investigation (FBI) and to submit entries and receive notification from the CRD.

Flight Crewmember: A pilot, flight engineer, or flight navigator assigned to duty in an aircraft during flight time.

Fingerprint Results Distribution (FPRD): TSA's secure web-based portal allowing an airport operator to review the Identify History Summary (IdHS) and complete the criminal history adjudication of covered individuals.

Individual: Individual who is applying for or holds airport operator-issued ID.

Identification (ID) Media ID: Media is any credential, card, badge, or other media issued for ID purposes and used at an airport. This includes, bus is not limited to, media signifying unescorted access to an Air Operations Area (AOA), Secured Area/SIDA, or Sterile Area**.**

Information Technology (IT) System: Any services, equipment, or interconnected systems(s) or subsystems(s) of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that fall within the responsibility of the airport operator to operate and maintain.

Indirect Air Carrier: Means any person or entity within the United States not in possession of an FAA air carrier-operating certificate that undertakes to engage indirectly in air transportation of property and uses for all or any part of such transportation the services of a passenger carrier. This does not include the United States Postal Service or its representative while acting on behalf of the USPS

Monitor: To observe the delivery of merchandise and consumables, in person or via closed-circuit television (CCTV), to ensure there is no unauthorized access to the merchandise or consumables. Monitoring may be performed by multiple personnel who have been trained to carry out this responsibility. Monitoring personnel must be capable of immediately initiating a response to any unauthorized access or activity near the merchandise or consumables, including immediately contacting laws enforcement or other local authority as appropriate.

Multi-factor Authentication: A physical access control system (PACS) operated by the airport operator which uses at least two of the following three factors of authentication:

- Something you have, such as a proximity card;
- Something you know, such as a Personal Identification Number (PIN);
- Something you are, such as a biometric comparison.

Operational Disruption: A deviation from or interruption of normal activities or operations that results in a loss of data, system availability, system reliability, or control of systems, or indicates unauthorized access to, or malicious software present on, critical information technology systems.

Physical Access Control System (PACS): A coordinated network of ID cards, electronic readers, field control panels, specialized databases, software, and computers designed, to monitor and control traffic through access points.

Private Charter: Means any aircraft operator flight- (1) For which the charter operator engages the total passenger capacity of the aircraft for the carriage of passengers; the passengers are invited by the charter operator; the cost of the flight is borne entirely by the charter operator and not directly or indirectly by any individual passenger; and the flight is not advertised to the public, in any way, to solicit passengers

Public Charter: Means any charter flight that is not a private charter

Quick Turn Flight: Flights where the foreign air carrier flight crewmembers or cabin crewmembers will not depart the Sterile Area before departing a U.S. airport, for example a flight from Canada, Mexico, or the Caribbean.

Reconciliation: Reconciliation is any process or procedure the airport operator conducts to reduce its rate of unaccounted-for ID media.

Rap Back: A program through FBI NGI that enables participating airport operators to receive ongoing status notifications of any subsequent criminal history information changes reported on covered individuals who have submitted fingerprints as part of a CHRC.

Revocation: The **final** cancellation (not including temporary suspensions) by the airport operator, **after exhausting the airport operator's hearing process**, of an individual's ID media due to a violation f an aviation security requirement.

Sterile Area Concessionaire: "Sterile Area Concessionaire Employee" means an employee of any entity that has an agreement with the airport operator to conduct business in the Sterile Area. Sterile Area concessionaire employees include employees of restaurants, specialty stores, and kiosks located within airport Sterile Areas. The term "Sterile Area Concessionaire Employee" does not include an employee of an airport operator, aircraft operator, or foreign air carrier that has a security program under 49 CFR Parts 1542, 1544 or 1546; this term also does not include Federal, Stat, or local government officials.

Scheduled Passenger Operations: Means an air transportation operation (a flight) from identified air terminals at a set time, which is held out to the public and announced by timetable or schedule, published in a newspaper, magazine or other advertising medium

Screening Functions: Means the inspection of individuals and property for weapons, explosives, and incendiaries

Screening Location: Means each site at which individuals or property are inspected for the presence of weapons, explosives, and incendiaries

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

Security Identification Display Area: SIDA means a portion of an airport specified in the airport security program, in which security measures specified in this part are carried out. This area includes the Secured Area and may include other areas of the airport

Sterile Area: Means a portion of an airport defined in the Kinexis Security Program that provides passenger's access to boarding aircraft and to which that access generally is controlled by TSA, or by an aircraft operator under Part 1544 of this chapter, through the screening of persons and property

Trusted Agent (TA): Means an individual(s) authorized as a representative of the airport and subject to the procedures outlined by the ASP and airport for the issuance of airport identification

(media). An airport operator employee or agent who collects information for a security threat assessment or criminal history records check (CHRC), transmits the information to a Designated Aviation Channeler, authorized the issuance of ID media, or issues ID media.

Unaccounted-For ID Media: Lost, stolen, or otherwise unrecovered ID media.

Unescorted Access Authority: Means the authority granted by an airport operator, an aircraft operator, foreign air carrier, or airport tenant under Part 1542, 1544, or 1546 of this chapter, to individuals to gain entry to, and be present without an escort in, Secured Areas and SIDA of airports

Unauthorized Access of an Information Technology (IT) System or Operational Technology System: Access from an unknown source; unauthorized access by a third party or former employee; an employee accessing systems for which they are not authorized; and may include a non-malicious airport operator policy violation such as the use of shared credential by an employee otherwise authorized to access it.

Unmanned Aircraft System (UAS): Unmanned Aircraft (UA) and associated elements (including communication links and components that control the UA) that are required for airport to operate safely and efficiently in the national airspace system. UA may also be referred to as a Drone, Unmanned Aerial Vehicle or Unmanned Aircraft Vehicle (UAV), and Remotely Piloted Aircraft (RPA).

Vetting Result: The instructions TSA issues to an airport operator for the purpose of defining an individual's watch list status.

AIRPORT INFORMATION

Mickey Mouse Airport (KMMW), also known as Micky Mouse Club House, is a public use airport located east of the central business district of Disney Corner, Florida. The airport is owned by the Disney Corner. Currently it operates two commercial airlines flights daily and serves general aviation activities as well.

The facility covers 1500 acres at an elevation of 4,250 feet above sea level above Disney Corner' city center. It has four runways with asphalt surfaces.

PART 1542 – AIRPORT SECURITY SUB-PART B 1542.103 (a) COMPLETE PROGRAM

CHAPTER - 1. AIRPORT SECURITY COORDINATOR §1542.3

In compliance with 49 CFR 1542.3, the Airport Security Coordinator (ASC) is responsible for the general administration of this Kinexis Security Program (ASP) and is identified in Section 1.1 below. Airport tenants, staff, or individuals with responsibilities under this plan will address all questions and comments concerning the ASP to the ASC.

This is position is critical for Airport Security.

Commented [SP1]: This is position is critical for Airport Security.

1.1. DESIGNATED ASC, ALTENRATE ASCs, AND MEANS OF CONTACT

The Airport will designate a primary ASC and an alternate ASC.

Designated Airport Security Coordinator (ASC)

The primary ASC is the Airport Operations Security Coordinator. The Airport Operations Security Coordinator is the primary contact for security-related activities and communications with the Transportation Security Administration (TSA). He is available 24 hours a day, 7 days a week. Refer to Appendix XL for details.

Alternate ASC and Means of Contact

The Supervisor of Airport Operations is the secondary Airport Security Coordinator. He serves as the secondary contact for security-related activities and communications with the TSA. He is available 24 hours a day, 7 days a week. Refer to Appendix XL for details.

1.2. RESPONSIBILITIES

The ASC serves as the Airport operator's 24-hour primary and immediate contact for security-related activities and communications with the TSA, FAA, and Airport tenants. The ASC also is charged with general oversight of Airport security functions, including managerial elements, as required to maintain Airport security under 49 CFR Part 1542. Additional responsibilities include, but are not limited to:

- Be available to TSA on a 24-hour basis.
- Review with sufficient frequency all security-related functions required of the Airport to ensure that all are effective and in compliance with 49 CFR 1542 ("Part 1542"), this Kinexis Security Program (ASP) document, and applicable Security Directives.

1.3. TRAINING REQUIREMENTS AND CURRICULUM

In accordance with 49 CFR Part 1542.3, the designated ASC, or alternate ASC, has successfully completed subject matter training to prepare the individual to assume the duties of the

position.

The Airport operator maintains the ASC training documentation until at least 180 days after the withdrawal of an individual designated as an ASC. The ASC training outline is attached in Appendix XH.

CHAPTER - 2. RESERVED

CHAPTER - 3. SECURED AREAS §1542.3

3.1. DESCRIPTION OF THE SECURED AREA

KMMW has one Secured Area. The Secured Area at KMMW as specified in this Airport Security Program, is where aircraft operators that have a security program under Parts 1544 or 1546 enplane and deplane passengers, sort, and unload baggage and in which certain security measures specified in Part 1542.201 are carried out. The Secured Area is adjacent to the sterile area of the passenger terminal area. Refer to Appendix C.

The Airport shall have the overall responsibility for the security of the Secured Area. In meeting this responsibility, the Airport shall, by the measures specified in this ASP, control access, movement of persons, and ground vehicles within the Secured Area, and promptly detect and take action to control each penetration or attempted penetration by unauthorized person. The Airport shall meet this responsibility in accordance with TSA regulations.

This is NOT SIDA.

Commented [SP2]: This is NOT SIDA.

3.2. SYSTEM, MEASURES, OR PROCEDURS USED TO CONTROL ACCESS TO THE SECURED AREA

In accordance with 49 CFR Part 1542.201, KMMW controls access to the Secured Area, controls the movement of individuals and vehicles within the Secured Area, and has established procedures to promptly detect and take action to control unauthorized access to the Secured Area. Access control measures at KMMW include lock & key with keys that are controlled and inventoried, cipher locks and electronic access-controlled card reader locks.

3.3.1 ACCESS CONTROL SYSTEM (ACS)

KMMW uses the Physical Access Control System (ACS). It is a comprehensive security solution designed to manage and control access to physical spaces within the Airport. All individuals requiring access to the Secured Area must possess, use, and visibly display an appropriate identification badge as described in Section X of this ASP. Individuals without Airport identification badges, who require access to the Secured Area, must be kept under escort.

As required by 49 CFR Part 1542.207(a), the measures in place at KMMW for controlling access to Secured Area of the Airport required under 49 CFR Part 1542.201(b)(1) will:

- Ensure that only those individuals authorized to have unescorted access to the Secured Area are able to gain entry.
- Ensure that an individual is immediately denied entry to a Secured Area when that person's access authority for that area is withdrawn; and
- Provide a means to differentiate between individuals authorized to have access to an entire Secured Area and individuals authorized access to only a particular portion of a Secured Area.

3.3.2 PERIMETER FENCING/ACCESS POINTS

Not applicable.

3.3.3 PERIMETER GATES/ACCESS POINTS

Not applicable. New gates at North side.

Commented [SP3]: New gates at North side.

3.3.4 SECURED AREA DOOR ACCESS PROCEDURES

Doors leading into the Secured Area from the Terminal and other facilities are controlled by at least one of the following: the access control system, lock & key, or alarms. Only those individuals with appropriate Airport-issued identification are authorized to access the Secured Area via a door. Authorized individuals are trained and instructed on push-pull (close) procedures to ensure SIDA doors are secured. Authorized individuals shall be held responsible and must ensure that no unauthorized or unescorted person follows them through the door. Refer to Appendix J for List of Access Points and Access Types.

3.3.5 BAGGAGE SYSTEMS

The baggage conveyance system located within the Terminal provides access to the Secured Area.

The system is equipped with locking devices that secure conveyance belt access to the Secured Area. Airline/Airport controlled bag belt doors are secured by electronic card access system with rollup-door mechanisms operated by authorized SIDA badge holder. Baggage conveyance systems are controlled by the Airport operations and monitored by respective airline tenants and TSA-contracted personnel using the system.

Aircraft operator baggage make-up activities are in the eastern side of the passenger terminal in the Secured Area.

3.3. SYSTEMS, MEASURES, OR PROCEDURES USED TO CONTROL ACCESS TO THE SECURED AREA

Unauthorized access to the Secured Area from the public area, AOA, or sterile area by persons or vehicles must be prevented, detected, and reported to the proper authorities. Checked baggage make-up areas which are included in the Secured Area, will be controlled to ensure unauthorized individuals are unable to access checked baggage.

Personnel identification media and ACS are described in Section 8. All individuals requiring access to the Secured Area must possess, use, and visibly display an appropriate identification badge. Additionally, all employees who maintain "unescorted access" to the SIDA, Secured Area, and/or AOA shall complete SIDA training, as described in Appendix F, before being granted unescorted access authority. Any individual without an airport identification badge who requires access to ramp areas must be kept under escort while in the Secured Area.

As required by 49 CFR Part 1542.207(a), the measures in place at KMMW for controlling access to Secured Area of the Airport required under 49 CFR Part 1542.201(b)(1) will:

- Ensure that only those individuals authorized to have unescorted access to the Secured Area are able to gain entry.
- Ensure that an individual is immediately denied entry to a Secured Area when that person's access authority for that area is withdrawn; and

3.4. CONTROL OF MOVEMENT WITHIN THE SECURED AREA

3.5.1 SECURITY RESPONSIBILITIES

It is the responsibility of every Airport-badged employee to conscientiously observe the presence of an Airport ID badge on another employee. Every Airport-badged employee is instructed that they must closely inspect the badge to ensure:

- The badge is valid for area of use.
- The badge has not expired.
- Photograph on badge matches employee.

Under no circumstance may an employee follow or allow another to follow through a card reader-operated door on the same card swipe. The only exception is the authorized escort of individuals utilizing the Airport's established escort procedures as described in Chapter 9.

An employee's Airport ID badge may not be given to another, or used by another, to work and/or gain entry through an airport badge-controlled door.

Under no circumstance may an employee's Airport-issued security key be given to or used by another employee to gain entry through an airport access-controlled door. Employees must ensure security access doors are secured after entry, and without allowing another

person to follow. Employees leaving the Secured Area and entering the Terminal Building must ensure that no one simultaneously exits the Terminal into the Secured Area.

3.5.2 PERSONAL RECOGNITION

All individuals requiring access to the Secured Area must possess, use, and visibly display an appropriate identification badge. Additionally, all employees who maintain "unescorted access" to the SIDA, Secured Area, and/or AOA shall complete SIDA training, as described in Appendix XJ, before being granted unescorted access authority.

3.5.3 CHALLENGE PROCEDURES

All individuals issued a badge permitting unescorted access to the Secured Area of the Airport shall be required to challenge any person(s) found not displaying a badge in the Secured Area/AOA. Details of the challenge procedure are defined in Chapter 10 of this ASP.

3.5.4 SECURITY SIGNAGE REQUIRED UNDER §1542.201(B)(6)

At each access point to the Secured Area, there are signs posted to warn individuals about the prohibition of unauthorized entry and all persons are subject to search. Signs warning individuals of parking restrictions must be posted at applicable locations where the parking of vehicles would interfere with the protection of the Secured Area. Refer to Appendix O.

CHAPTER - 4. AIR OPERATIONS AREA (AOA) §1542.203

4.1 DESCRIPTION OF THE AIR OPERATIONS AREA

Airport Operations Area (AOA) at KMMW is the portion of the airport, specified in the Airport Security Program, in which security measures specified in 49 CFR Part 1542 are performed. This area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas, for use by aircraft regulated under 49 CFR Part 1544 or 1546, and any adjacent areas (such as general aviation areas) and areas within the perimeter fence that are not separated by adequate security systems, measures, or procedures. The AOA is any other area within the perimeter fence that is not included in the Secured Area. This includes operating areas leased by airport tenants and other aeronautical users. A map of the AOA at KMMW is shown in Appendix D.

4.2 SYSTEMS, MEASURES, OR PROCEDURES USED TO PERFORM THE ACCESS CONTOL FUNCTIONS REQUIRED UNDER §1542.203

The systems, methodologies, and procedures contained herein for the ACS system at KMMW meet the requirements of 49 CFR Part 1542.207(c).

KMMW is responsible for the security of the AOA. In meeting this responsibility, the airport shall control access to the AOA, control movement of persons and ground vehicles within the AOA, and promptly detect and take action to control each penetration, or attempted penetration of the AOA by unauthorized persons.

4.2.1 ENHANCED ACCESS MEDIA CONTROL

The systems, methodologies, and procedures contained herein for the ACS system at KMMW meet the requirements of 49 CFR Part 1542.207(c). KMMW uses the same access control infrastructure, software, and methods to protect the AOA that are used in the Secured Area.

4.2.2 KEY CONTROL/CIPHER CODES

The Airport shall maintain a positive lock and key control system. Padlocks are used on Airport-controlled AOA gates and access points.

4.2.3 ACCESS CONTROL SYSTEM AUDITS

The Airport shall conduct an annual AOA badge and key audit to ensure that all Airport-issued access media are accounted for. The access control system and associated databases are controlled by computer systems, access to these systems are controlled by personalized user access credentials.

CHAPTER - 5. SECURITY IDENTIFICATION DISPLAY AREA (SIDA) §1542.205

The SIDA is a portion of an airport, specified in this security program, in which security measures specified in this part are carried out. The "SIDA" is defined as that area identified as requiring that each person shall continuously display on their outermost garment, above waist level, the airport-approved identification medium, unless that person is under airport-approved escort.

CHAPTER - 6. STERILE AREA §1542.103

6.1 DESCRIPTION OF THE STERILE AREA

The Sterile Area is that portion of the Airport that provides passenger access to boarding aircraft and to which access is controlled by the TSA through the screening of individuals and property.

The Sterile Area at KMMW includes the passenger-screening checkpoint controlled by the TSA or its contracted agent, and the ticketed passenger hold room and restrooms beyond the passenger-screening checkpoint. See Appendix A for a map of the Sterile Areas at KMMW.

CHAPTER - 7. PROCEDURES USED TO COMPLY WITH §1542.209 REGARDING FINGERPRINT-BASED CRIMINAL HISTROY RECORDS CHECKS, SECURITY THREAT ASSESSMENTS, AND CENTRALIZED REVOCATION DATABASE

Each individual requesting unescorted access authority at KMMW Sterile Area, Secure Area, (Passenger Concourse), and/or SIDA is required to be cleared of the disqualifying criminal offenses per CFR 1542.209(d) by undergoing a biometric (fingerprint) Criminal History Records Check (CHRC). In addition, and in compliance with the Security Directive 1542-04-08 series, the Airport does not issue any type of Airport ID Badge until the TSA has completed a Security Threat Assessment (STA) on an individual and determined that the individual has a favorable result.

CHAPTER - 8. DESCRIPTION OF THE PERSONNEL IDENTIFICATION SYSTEM §1542.211

KMMW provides for a personnel identification system that meets the requirements of §1542.201(b)(3) and §1542.205(b)(1). Each person who has Airport-authorized unescorted access to or within the Secured Area and/or AOA is issued one card, which serves the dual purposes of identification and area access.

8.1 THE PERSONNEL IDENTIFICATION SYSTEM

KMMW uses the following procedures to secure the means by which the identification media are issued. These include:

- Issuing ID media with a 5-year expiration date.
- Physically retrieving expired identification media of individuals who no longer have unescorted access authority.
- Requiring holders of media and their respective employers to immediately report lost or stolen media.
- Securing all blank identification media stock and supplies.

Random ID Media Audit

The airport operator will conduct a random ID media audit, using one of the audit types listed in Section II., starting on a TSA-Approved Kinexis Security Program Amendment ABCD-PP-1919-102.

KMMW will notify the FSD or designee in writing of the date the random ID media audit will start, no less than 5 calendar days prior to the start of the random ID media audit.

8.2 IDENTIFICATION SYSTEM

KMMW-issued security identification media (badges) ensure appropriate access restrictions through programmable electronic means (access control system) and procedure by ensuring that all badged personnel are properly trained. The media are sized per §1542.211

regulations and are configured or manufactured in a manner that reasonably discourages duplication and counterfeiting.

Airport-issued Identification Media (ID Badges)

Front of Identification Media:

- Airport logo (3-letter code)
- Conveys a full-face photo, name, employer, and the unique identification badge number of the individual to whom the medium is issued;
- Clearly indicates the badge type indicating an individual's access and movement privileges;
- Indicates expiration date, a minimum of one quarter inch in height (AP 97-01);
- Is of sufficient size and appearance as to be readily observable for challenge purposes;

Back of Identification Media Includes:

- Airport's return address and phone number;
- Security Notification/Property of KMMW

Endorsements:

1. Escort privileges endorsement:
   ESCORT Driver privileges endorsements:
   MOVEMENT —
   NON- MOVEMENT —

KMMW badge samples are shown in Appendix E.

8.3 SECURITY IDENTIFICATION MEDIA DISPLAY AND ESCORT

All individuals within the Sterile, Secure and SIDA areas will display on their person, at all times, the KMMW-issued media, or other accepted forms of identification. The Airport ID media must be displayed on the outermost garment, above the waist, and below the neck. AII individuals with official business who are in a SIDA, Secure, or AOA, that do not possess an ID media approved in this chapter must be under proper escort. See Chapter 9 for escort procedures.

CHAPTER - 9. ESCORT PROCEDURES §1542.211 (e)

KMMW shall follow the procedures described in §1542.211 for those persons requiring unescorted access to the Sterile Areas, Secured Areas, AOA or the SIDA. Individuals who have

the authority to escort persons into Sterile Areas, Secured Areas, AOA or the SIDA are only granted such authority after the following:

- A written request from a company's signatory must be submitted and approved by the Airport Security Coordinator (ASC) for escort privileges.
- A copy of the approved Signatory Authorities' request for designated escort authority must be on file with the Airport Badging Office prior to issuing a designated escort ID media. The individual receiving the ID media must be specifically identified on the request letter including the business need for conducting escorts.

CHAPTER - 10. CHALLENGE PROCEDURES §1542.211 (d)

KMMW will enforce challenge procedures in accordance with §1542.211(d).

When an individual fails to produce Airport-issued ID media or is not under proper escort, then that person must be escorted from the SIDA, AOA or Secure Area and Airport Operations must be notified.

CHAPTER - 11. TRAINING PROGRAMS REQUIRED UNDER §1542.213 AND §1542.217(c)(2)

KMMW ensures that performing security-related functions for the Airport are trained on the provisions of this Part, Security Directives, Information Circulars, and the Airport Security Program, to the extent that such individuals that have a need to know in order to perform their duties. This is accomplished through individual Training, Security briefings, and Notification to stakeholders.

The Airport does not authorize any individual unescorted access to the Secured Area, Security Identification Display Area (SIDA), Airport Operations Area (AOA) or Sterile Area, unless that individual has successfully completed training in accordance with an approved curriculum. The method of instruction shall be based upon TSA-approved curriculum as required by 49 CFR Part 1542.213 delivered via computer-based secured Internet access providing for instruction and testing or via classroom training with KMMW-specific handout materials.