Section 2: To be completed by applicant

Please print clearly. Do not leave spaces blank. If an area not applicable – Write N/A

Section 2:

Applicant Information:

Notice: All applicants are required to undergo a CHRC and STA before access may be granted

Full Legal Last Name:
Full Legal First Name:
Full Legal Middle Name:

Required: Alias/Other Names Used Legally (former name, maiden name)
Last:
First:
Middle:

Phone Number:	**Social Security Number:**

Sex:	**Ethnicity:**	**Height: ’ ”**	**Weight (lbs):**	**Hair Color:**	**Eye Color:**	**Date of Birth: MM/DD/YYYY**

Place of Birth (State and/or Country):			
Current Mailing Address:			
City:	**State:**	**Zip Code:**	**Country:**

Citizenship Country Code:	**Passport Country:**	**Passport #:**	**Cert. of Naturalization #:**
Cert. of Birth Abroad (DS 1350/FS-240/ FS-545) #:	**Alien Registration #:** **Date of Expiration:**	**Non-Immigrant Visa #: (Top right corner)**	**I94 Arrival/Departure Form #: (11 digits)**

Company or Tenant Name:	**PIN-3, 4, digits. Must be done in ASO**	**Applicant Position:**

Section 3: To be completed by applicant

Section 3:

Criminal History Record Check (CHRC)/Fingerprint Questionnaire Disqualifying Crimes List:

During the previous years have you been convicted or found not guilty by reason of insanity of any of the crimes listed below? ☐ Yes ☐ No

If your answer to the question above is yes, please check the box next to each offence that applies:

☐ Forgery of certificates, false marking of aircraft, and other aircraft registration violation;

☐ Interference with air navigation;

☐ Improper transportation of a hazardous material;

☐ Aircraft piracy;

☐ Interference with flight crew members or flight attendants;

☐ Commissions of certain crimes aboard aircraft in flight;

☐ Carrying a weapon or explosive aboard aircraft;

☐ Conveying false information and threats;

☐ Aircraft piracy outside the special aircraft jurisdiction of the United States;

☐ Lighting violations involving transporting controlled substances;

☐ Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements;

☐ Destruction of an aircraft or aircraft facility;

☐ Murder;

☐ Assault with intent to murder;

☐ Espionage;

☐ Sedition;

☐ Kidnapping or hostage taking;

☐ Treason;

☐ Rape or aggravated sexual abuse;

☐ Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon;

☐ Extortion;

Section 3 Continued:

- ☐ Armed or felony unarmed robbery;
- ☐ Distribution of, or intent to distribute, a controlled substance;
- ☐ Felony arson;
- ☐ Felony involving a threat;
  Felony involving –
- ☐ Willful destruction of property;
- ☐ Importation or manufacture of a controlled substance;
- ☐ Burglary;
- ☐ Theft;
- ☐ Dishonesty, fraud, or misrepresentation;
- ☐ Possession or distribution of stolen property;
- ☐ Aggravated assault;
- ☐ Bribery; or
- ☐ Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year;
- ☐ Violence at international airports;
- ☐ Conspiracy or attempt to commit any of the criminal acts listed in this paragraph

Federal regulations under 49 CFR 1542.209(1) impose a continuing obligation to disclose to the airport operator within 24 hours if you are convicted of any disqualifying offense that occurs while you have unescorted access authority.

I certify that I do not have any of the above disqualifying crimes and the information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement on this application can be punished by fine or imprisonment or both. I understand I may receive a copy of the criminal record received from the FBI if requested in writing and that my point of contact should I have any questions about the results of the CHRC is the Airport Security Coordinator (ASC).

Printed Name of Applicant	Signature of Applicant	Date

Section 4: To be completed by applicant

Section 4:

Screening Notice:

For all SIDA ID media applicants
"Any employee holding a credential granting access to a Security Identification Display Area may be screened at any time while gaining access to, working in, or leaving a Security Identification Display Area." **Initial** _____

Section 5: To be completed by applicant

Section 5:

Biometric Data Notice and Acknowledgment:

Biometric Data Notice:

TAA uses biometric facial technology as part of its access control and airport security programs to verify an individual's identity during badge enrollment, renewal, replacement, or use; authenticate the identity of an authorized badge holder; control or verify access to restricted or secured areas; and detect and prevent unauthorized use of airport credentials. As a condition of obtaining and maintaining a TAA-issued SIDA badge and associated access control privileges, an applicant must participate in TAA's biometric facial authentication process.

Biometric facial technology creates or uses a mathematical representation, template, or other biometric identifier derived from an individual's facial image ("biometric data") to identify that individual through comparison against an authorized security database. Biometric facial authentication technology does not collect any Personally Identifiable Information (PII).

TAA will not sell, lease, trade, or use biometric data for advertising, marketing, or other unrelated commercial purposes. Biometric data processors may access biometric data when reasonably necessary to operate or support TAA's biometric data program. TAA may be obligated to disclose biometric data when required under applicable federal or state law, regulation, court order, warrant, or applicable FAA or TSA security requirement.

TAA will maintain reasonable administrative, technical, and physical safeguards of biometric data. Biometric data will be retained for so long as reasonably necessary to accomplish the purpose for which it was collected, or for such period as required by applicable law. TAA will dispose of the biometric data in accordance with applicable law.

Section 5 Continued:

Biometric Data Acknowledgments:

I have read the Biometric Data Notice and consent to TAA, or its authorized biometric data processors, collecting, generating, processing, storing, and using my biometric data as stated in the Notice. **Initial** _____

I understand that failure or refusal to provide biometric data or participate in biometric data screening will result in denial or suspension of SIDA badge and associated access privileges. **Initial** _____

Section 6: To be completed by applicant

Section 6:

TSA Privacy Act Statement:

Authority: 6 U.S.C. § 1140, 46 U.S.C. § 70105; 49 U.S.C. §§ 106, 114, 5103a, 40103(b)(3), 40113, 44903, 44935-44936, 44939, and 46105; the Implementing Recommendations of the 9/11 Commission Act of 2007, § 1520 (121 Stat. 444, Public Law 110-53, August 3, 2007); FAA Reauthorization Act of 2018, § 1934(c) (132 Stat. 3186, Public Law 115-254, Oct 5, 2018), and Executive Order 9397 (November 22, 1943), as amended.

Purpose: The Department of Homeland Security (DHS) will use the information to conduct a security threat assessment. If applicable, your fingerprints and associated information will be provided to the Federal Bureau of Investigation (FBI) for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems including civil, criminal, and latent fingerprint repositories. The FBI may retain your fingerprints and associated information in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI. DHS will also transmit your fingerprints for enrollment into US-VISIT Automated Biometrics Identification System (IDENT).

DHS will also maintain a national, centralized revocation database of individuals who have had airport- or aircraft operator- issued identification media revoked for noncompliance with aviation security requirements. DHS has established a process to allow an individual whose name is mistakenly entered into the database to correct the record and have the

Section 6 Continued:

individual's name expunged from the database. If an individual who is listed in the centralized database wishes to pursue expungement due to mistaken identity, the individual must send an email to TSA at aviation.workers@tsa.dhs.gov.

Routine Uses: In addition to those disclosures generally permitted under 5 U.S.C. § 522a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 522a(b)(3) including with third parties during the course of a security threat assessment, employment investigation, or adjudication of a waiver or appeal request to the extent necessary to obtain information pertinent to the assessment, investigation, or adjudication of your application or in accordance with the routine uses identified in the TSA system of records notice (SORN) DHS/TSA 002, Transportation Security Threat Assessment System. For as long as your fingerprints and associated information are retained in NGI, your information may be disclosed pursuant to your consent or without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses.

Disclosure: Pursuant to § 1934(c) of the FAA Reauthorization Act of 2018, TSA is required to collect your SSN on applications for Secure Identification Display Area (SIDA) credentials. For SIDA applications failure to provide this information may result in denial of a credential. For other aviation credentials, although furnishing your SSN is voluntary, if you do not provide the information requested, DHS may be unable to complete your security threat assessment. **Initial** _____

Part 1520 – Protection of Sensitive Security Information:
I have received "Part 1520- Protection of Sensitive Security Information."
(Will be given from ASO) Initial _____

TSA (FAA) Security Directive AP 97-01, Is Still In Effect And Requires That . . .
All personnel, air carriers and tenants, sub-tenants, contractors, etc. provide immediate notification to the Tucson Airport Authority when an individual's access authority has been revoked or limited; lost or stolen; or the air carrier or tenant becomes aware the access control system, or a component of the system, has been compromised or threatened through any means. You may contact any Tucson Airport Police personnel, or you may phone the TAA Communications Center at 520-573-8182 to report any of the above information. **Initial** _____

Section 7: To be completed by applicant

Section 7:

Certifications:

Purposes of SSN verification

"I authorized the Social Security Administration to release my Social Security Number and full name to the Transportation Security Administration, Intelligence and Analysis (IA), Attention: Aviation programs (TSA-10)/Aviation Worker Program, 601 South 12th Street, Arlington, VA 20598."

"I am the individual to whom the information applies and want this information released to verify that my SSN is correct. I know that if I make any representation that I know is false to obtain information from Social Security records, I could be punished by a fine or imprisonment or both."

"The information I have provided is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement can be punished by fine or imprisonment or both (see Section 1001 of Title 18 of the United States Code)."

Signature of Applicant	Date of Birth	SSN and Full Name Printed
Must be done in ASO	Must be done in ASO	Must be done in ASO

ASO Use Only

Badge Processing Status/General Requirements

TAA may not issue identification media to an applicant or grant privileges that accompany issuance of the identification media until TAA has verified the identity and work authorization of the applicant as set forth in section lll prior to submitting biographical information to TSA for an STA.

IET Information Entered	Date:	Trusted Agent:
Identity and Work Authorization Verified	Date:	Trusted Agent:
Fingerprints (CHRC) Submitted	Date:	Trusted Agent:
Picture Taken	Date:	
Biometric Facial Image Captured	Date:	
Enrolled in Rock facial authentication	Date:	
STA Information Entered	Date:	Trusted Agent:
ID Media Number:		
Access Level (SIDA, AOA, Sterile):		
Access Template:		
CHRC Clearance	Date:	Trusted Agent:
CHRC Denied	Date:	Trusted Agent:
STA Clearance	Date:	Trusted Agent:
SIDA Completion	Date:	
Driver Completion	Date:	
ID Media Issued	Date:	Trusted Agent:
TAA Essential Critical Infrastructure Worker Badge	Date:	
TAA Prox Card	Date:	