

# Airport ID Badge Application

AOA Badge

## Identity

Last Name \_\_\_\_\_ First Name \_\_\_\_\_

Middle Name \_\_\_\_\_ Suffix \_\_\_\_\_ SSN \_\_\_\_\_

Alias/Other Names Used-Include Maiden Name \_\_\_\_\_

Date of Birth \_\_\_\_\_ Country of Birth \_\_\_\_\_

Citizenship \_\_\_\_\_ State/Province of Birth \_\_\_\_\_

## Contact Information

Address \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

Primary Phone \_\_\_\_\_ Mobile Phone \_\_\_\_\_

Email \_\_\_\_\_

## Characteristics

Height \_\_\_\_\_ (ft) \_\_\_\_\_ (in) Weight \_\_\_\_\_ (lbs) Gender \_\_\_\_\_

Eye Color \_\_\_\_\_ Hair Color \_\_\_\_\_ Ethnicity \_\_\_\_\_

## Government ID

Primary ID Type \_\_\_\_\_ ID Number \_\_\_\_\_

Expiration Date \_\_\_\_\_ Country Issued \_\_\_\_\_ State \_\_\_\_\_

## Secondary ID

Secondary ID Type \_\_\_\_\_ ID Number \_\_\_\_\_

Expiration Date \_\_\_\_\_ Country Issued \_\_\_\_\_ State \_\_\_\_\_

Two pieces of valid, original, unexpired and legible documentation are required. Copies will not be accepted. At least one identification document must include a photo. Applicant must provide documentation that establishes both identity and employment eligibility. Non-US citizens and US citizens born abroad will require additional documentation. For more information on acceptable ID's, visit [www.uscis.gov/i-9-central](http://www.uscis.gov/i-9-central).

## Authorized Signer

Applicant Name \_\_\_\_\_

Job Title \_\_\_\_\_

Badge Sponsor \_\_\_\_\_

Company Name (if different from sponsor) \_\_\_\_\_

Transaction Type	New Badge	Renewal	Replacement Badge
Badge Type	AOA	Flight School AOA	
Endorsements	Escort	Movement Area Driver	Non-movement Area Driver

## Employers Certification

By signing this application, I certify that a specific need exists for providing the individual applicant with unescorted access authority. The information provided on this application is true 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 (Section 1001 Title 18 USC).

I have physically inspected the identification documents listed on this application and have informed the applicant that they must present the documents to the airport badge office.

I have explained and the applicant acknowledges their security responsibilities listed in 49 CFR Part 1540.105(A):

### *49 CFR Part 1540.105(A)*

- (1) Tamper or interfere with, compromise, modify, attempt to circumvent, or cause a person to tamper or interfere with, compromise, modify, or attempt to circumvent any security system, measure, or procedure implemented under this subchapter.*
- (2) Enter, or be present within, a secured area, AOA, SIDA or sterile area without complying with the systems, measures, or procedures being applied to control access to, or presence or movement in, such areas.*
- (3) Use, allow to be used, or cause to be used, any airport-issued or airport-approved access medium or identification medium that authorizes the access, presence, or movement of persons or vehicles in secured areas, AOA's, or SIDA's in any other manner than that for which it was issued by the appropriate authority under this subchapter.*

## Authorized Signatory

Printed Name \_\_\_\_\_ Date \_\_\_\_\_

Company \_\_\_\_\_

Signature \_\_\_\_\_

## Applicant Certification

I authorize the Social Security Administration to release my Social Security Number and full name to the Transportation Security Administration, Enrollments Services and Vetting Programs, Attention: Vetting Programs (TSA-10)/Aviation Worker Program, 6595 Springfield Center Drive, Springfield, VA 20598-6010.

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.

Initials \_\_\_\_\_

## 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 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](mailto:Aviation.workers@tsa.dhs.gov).

- **Routine Uses:** In addition to those disclosures generally permitted under 5 U.S.C. § 552a(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. § 552a(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 will 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.

Initials \_\_\_\_\_

## Airport use of Personally Identifiable Information

In addition to the above uses for Department of Homeland Security, all Personally Identifiable Information (PII) including contact information, biographical information, and biometric information (which may include but is not limited to fingerprints, iris scan, retina scan, hand geometry, etc.) collected by the Airport will be used for Airport security and operational purposes. Uses include but are not limited to Department of Homeland Security required fingerprint based criminal history records checks which includes perpetual vetting, TSA Security Threat Assessment, and for other record checks including but not limited to searches for valid driver's license and active arrest warrants. Biometric information will also be used for access and identification within the Airport's credentialing and access control system. Contact information including mailing address, email address, phone, cell phone, and text messaging will be used by the Airport to communicate information regarding airport security, airport operations, airport safety, airport ID badging, billing or financial transactions, and important information regarding airport operational incidents and/or emergencies.

Initials \_\_\_\_\_

## True and Correct Statement

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 (Section 1001 of Title 18 of the United States Code).

Initials \_\_\_\_\_

Applicant Full Name \_\_\_\_\_ SSN \_\_\_\_\_

Signature \_\_\_\_\_ Date of Birth \_\_\_\_\_