



ID BADGE RENEWAL/REPLACEMENT FORM

EMPLOYEE

Company Name: _____ Badge Number: _____

Last Name: _____ Suffix: _____ First Name: _____ MI: _____

Social Security Number: _____ - _____ - _____ Date of Birth (mm/dd/yyyy): _____ / _____ / _____

Country of Birth (country name): _____ City and State of Birth: _____

Current Mailing Address: _____ City: _____

County: _____ State: _____ Zip Code: _____ Contact Phone Number _____ - _____ - _____

Electronic Mail Address (e-mail) (Optional): _____ @ _____

MY SIGNATURE BELOW ACKNOWLEDGES THE FOLLOWING:

I acknowledge receipt of a SIDA badge and will adhere to the "Airport Rules and Regulations" as required by the TSA and Department of Aviation. I understand that it is a violation of Airport Rules and Regulations to lend, alter, or change a SIDA badge in any way. The SIDA badge is the sole property of the Department of Aviation and must be returned upon separation from employment, or upon demand of the Department of Aviation. My signature acknowledges that I have successfully completed IET based SIDA Training for Philadelphia Int'l Airport, required under 49 CFR 1542.213.

- Lost/Stolen badges must be reported to DOA-SECURITY within 24hrs. Failure to do so is a violation of Airport Rules and Regulations. DOA-SECURITY can be reached 24/7 by calling 215-937-5452 or 4444 from a white phone.
- Fees for lost, stolen, and damaged badges are as follows:
 - 1st Occurrence - \$100. 2nd Occurrence - \$150. 3rd Occurrence - \$200. 4th Occurrence - Possible Revocation.
 - Fees for stolen badges will be waived upon receipt of official police report.
 - **TWO forms of ID are ALWAYS required when obtaining a new badge.**

Privacy Act Notice:

Authority: 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, as amended.

Purpose: The Department of Homeland Security (DHS) will use the biographic information to conduct a security threat assessment. 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 may provide your name and SSN to the Social Security Administration (SSA) to compare that information against SSA records to ensure the validity of the information.

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. 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)

I authorize the Social Security Administration to release my Social Security Number and full name to the Transportation Security Administration, Enrollment Services and Vetting Programs, Attention: Aviation 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.

Employee Signature: _____ Date: _____ / _____ / _____

SCREENING NOTICE: 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.

ID BADGE RENEWAL/REPLACEMENT FORM

EMPLOYER (TO BE COMPLETED BY AUTHORIZED SIGNER)

Employee Name: _____ Badge #: _____

Company: _____

Badge Type: RENEWAL UPGRADE / DOWNGRADE LOST / DAMAGED / STOLEN OTHER*

*DESCRIPTION _____

The employee's job duties require access to the following security areas:

- BLUE** – All Secured and AOA areas including terminals. Valid for two (2) years.
- BLACK** – All Secured and AOA areas including terminals. Valid for one (1) year.
- YELLOW** – Temporary Contractors badge All Secured and AOA areas including terminals. Valid for one (1) year.
- RED** – Sterile Area access located beyond the passenger screening checkpoint(s). Valid for two (2) years.

Authorized Signer Clause:

As the employer & Authorized Signer of the above listed individual, I understand it is my responsibility to verify the information on this renewal form. As the Authorized Signer I am also responsible for ensuring that my employees follow all applicable rules set forth in the Airport Security Program and in the Airport Rules & Regulations Guide. I understand that it is my responsibility to disclose any known security breach committed by any of my employees and any known criminal arrests or criminal convictions to the Airport Security Coordinator or their authorized designee. Failure to do so may result in temporary or permanent revocation of the employee's security access and all applicable fines being assessed against me or my company and the possible loss of Authorized Signer Status and termination of all contracts and leases with the Department of Aviation.

(Air Carrier Only), I certify that, if the results of a CHRC or RBN disclose a conviction for a disqualifying criminal offense in accordance with 49 CFR 1542.209, the aircraft operator must notify DOA – Security within 24hrs. If information becomes available to DOA-Security indicating that an individual with unescorted access authority has a disqualifying criminal offense, DOA – Security will conduct a CHRC investigation on that individual.

Authorized Signer (print) _____ Contact #: _____

Authorized Signature: _____ Date: _____

Email (Required): _____

CHRC CERTIFICATION (AIR CARRIER ONLY)

CHRC CASE #: _____ FBI#: _____ DATE: _____

DOA-SECURITY

RapBack Enrollment Successful (Y/N): _____ DATE: _____ CHRC CASE #: _____ FBI#: _____

Company Code/Bill Class _____ Issue Date: _____ Expire Date: _____

Trusted Agent Initials: _____