Privacy Act Notice

The Transportation Security Administration (TSA) requires that all badge applicants be apprised of various privacy laws. The following language is required by the TSA:

Authority: Title 6 of the United States Code (U.S.C.), section 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); the *FAA Reauthorization Act of 2018*, §1934(c), (i) (132 Stat. 3186, Public Law 115-254, Oct 5, 2018), and Executive Order 9397, as amended.

Purpose: The U.S. Department of Homeland Security (DHS) will use the biographic and biometric information to conduct a security threat assessment. Your fingerprints and associated information will be provided to the Federal Bureau of Investigation (FBI). The FBI will compare your fingerprints to other fingerprints in its Next Generation Identification (NGI) system or its successor systems including civil, criminal, and latent fingerprint repositories. The FBI may keep your fingerprints and associated information in NGI after the completion of this application and continue to compare them against other fingerprints submitted to or kept by NGI. DHS will also send your fingerprints for enrollment into the DHS Automated Biometrics Identification System (IDENT).

DHS will also maintain a national, centralized revocation database. This database will contain the names of individuals who have had airport-issued identification (ID) media revoked for not complying with aviation security requirements. This information will remain in the revocation database for five (5) years from the date the badge was revoked. Individuals who believe their name is mistakenly entered in the database can ask for the record to be corrected and have their name removed from the database by following the aircraft or airport operator's redress procedures.

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 under 5 U.S.C. 522a(b)(3). Routine use includes those uses identified in the TSA system of records notice DHS/TSA 002, Transportation Security Threat Assessment System. It also includes disclosures to third parties during a security threat assessment, employment investigation, or adjudication of a waiver or appeal request as necessary to get information relevant to assessing, investigating, or adjudicating your application.

For as long as your fingerprints and associated information are kept in NGI, your information may be disclosed with your consent or without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses.
DHS may provide your name and social security number (SSN) to the Social Security Administration (SSA) to validate that information against SSA records.

Disclosure: Under section 1934(c) of the *FAA Reauthorization Act of 2018*, TSA must collect your SSN on applications for Secure Identification Display Area (SIDA) credentials. If you do not provide this information, TSA will deny your request for a SIDA credential. Although providing your SSN is voluntary for other aviation credentials, if you do not provide it, DHS may be unable to complete your security threat assessment.