CHRC / Privacy Act Certification

(Regulated Airlines)

The certification below must be initiated and ultimately completed for all applicants prior to the issuance or replacement of an airport badge. The company signature authority must verify that the applicable TSA Security Directive requirements have been performed prior to issuance of the airport media (badge). The new CHRC date that will be entered into the HAS Security Badging application will be the "Date Received" for normal CHRC processing or "Date Enrolled" for the RAP Back program as indicated in the certification statement below.

"I certify that a Criminal History Records Check has been completed on this applicant by the appropriate Federal agency and does not disclose a disqualifying conviction as described in 49 CFR Part 1542.209, 1544.229 or 1544.230. A copy of the Privacy Act has been provided to the applicant." (for Government and Regulated entities)

CHRC Case # _____ | _____ | _____

Date Submitted | **Date Received**

or

RAP Back _____ | _____ | _____

CHRC Case # | **Date Enrolled**

Application Date: _____ (no earlier than 60 days prior to badge expiration date)

Applicant Name: _____

Employer Name: _____

Signature Authority: _____ _____

Signature | **Date**

_____

Print Name

The Privacy Act of 1974
5 U.S.C. 552a(e)(3)

Privacy Act Notice

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). If you provide your Social Security Number (SSN), 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 pe1mitted 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, Transp01tation 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: Furnishing this information is voluntary; however, if you do not provide the information requested, DHS may be unable to complete your application for a security threat assessment.