



Syracuse Hancock International Airport ID/Access Media Application

Badge Access/Color:

SECURED: [] Yellow AOA ONLY: [] Green STERILE ONLY: [] White

Fingerprint Date: _____

Badge Number: _____

Fingerprint Approved Date: _____

LEO Endorsement: [] Yes [] No

Fingerprint Case #: _____

Escort Endorsement: [] Yes [] No

FP Case # Verified By: _____

Vehicle Endorsement: [] Non-Movement [] Movement

STA: [] Pass [] Fail Date: _____

SIDA Training Completed on _____ Verified by: _____

STA Verified by: _____

Customs Endorsement: [] Yes [] No

TA who collected the biographical and biometric information used in CHRC/STA & verifies ID _____

TA that transmitted STA/CHRC _____ TA who issued ID Media _____

TA who authorized the issuance of the ID Media _____ Date Issued _____

Acceptable Documents Provided by Applicants

Airport operators must not issue any type of SIDA identification media that allows unescorted access until the information requested in this application is submitted to TSA and the TSA has completed a Security Threat Assessment (STA) on the individual and determined that the individual does not pose a threat to security.

All applicants must provide a document from List A or document from List B & C. If the applicant is a TSA or other Non-LEO Federal employee, they can provide their agency documentation. (Reference I-9 form)

Item from List A: _____ Number _____ EXP _____ Verified _____

Item from List B: _____ Number _____ EXP _____ Verified _____

Item from List C: _____ Number _____ EXP _____ Verified _____

TSA or Non-LEO Federal Employee Agency ID: _____ EXP _____ Verified _____

Security Use Only

Section I – Applicant (This section must be typed or in print)

Last Name _____ First Name _____ Middle Name _____
Aliases _____
Other Names Used _____ (former name, maiden name, nickname)
Street Address _____
City/State/Zip _____
Phone Number _____ Gender Male Female Race _____
Date of Birth ____/____/____ Place of Birth _____ Country _____
MM DD YYYY
Citizenship _____ Social Security Number _____ -- -- -- --
If Not a US Citizen Do You Have an Employee Authorization to Work in the US yes no Expiration Date _____
Hair Color _____ Eye Color _____ Height _____ Weight _____
Employer _____ Job Title _____ Date of Hire _____
Employer Address _____

Section II – Criminal History

49 CFR Parts 1542 and 1544 and Public Law #106-528 prohibit anyone who has been convicted or found not guilty by reason of insanity within the previous 10 years of the following crimes from being granted unescorted access to the airport's Security Identification Display Area (SIDA). That is, that person may not be given/issued an airport badge. All applicants must submit fingerprints which will be used to check the person's criminal history records. The list below is from 49 U.S.C 44936(b)(1)(B) United States Code and 49 C.F.R. 1554.229(d).

- | | |
|--|--|
| 1. Forgery of certificated, false marking of aircraft, and other aircraft registration violations | 20. Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon |
| 2. Interference with air navigation | 21. Extortion |
| 3. Improper transportation of a hazardous material | 22. Armed or felony unarmed robbery |
| 4. Aircraft Piracy | 23. Distribution of, or intent to distribute, a controlled substance |
| 5. Interference with flight crew members or flight attendants | 24. Felony arson |
| 6. Commission of certain crimes aboard aircraft in flight | 25. A felony involving a threat |
| 7. Carrying a weapon or explosive aboard an aircraft | 26. A felony involving the willful destruction of property |
| 8. Conveying false information and threats | 27. A felony involving importation or manufacture of a controlled substance |
| 9. Aircraft Piracy outside the special aircraft jurisdiction of the United States | 28. A felony involving burglary |
| 10. Lighting violations involving transporting controlled substances | 29. A felony involving theft |
| 11. Unlawful entry into an aircraft or airport area that serves carriers of foreign air carriers contrary to established security requirements | 30. A felony involving dishonesty, fraud, or misrepresentation |
| 12. Destruction of an aircraft or aircraft facility | 31. A felony involving possession or distribution of stolen property |
| 13. Murder | 32. A felony involving aggravated assault |
| 14. Assault with intent to murder | 33. A felony involving bribery |
| 15. Espionage | 34. A felony involving illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than one year |
| 16. Sedition | 35. Violence at international airports |
| 17. Kidnapping or hostage taking | 36. Conspiracy or attempt to commit any of the aforementioned criminal acts |
| 18. Treason | |
| 19. Rape or aggravated sexual abuse | |

The Airport Security Coordinator keeps confidential criminal history records obtained from the FBI and uses them only for determining whether to issue an airport badge. You may get a copy of your criminal history records sent to the FBI to the Airport Security Coordinator by submitting a written request within 30 days of being advised that your criminal history disqualifies you from being issued an airport badge. If you believe that any information is inaccurate, you may directly contact the agency that reported the disqualifying conviction to correct your record.

I have read the list of Disqualifying Criminal Offenses and certify that I have not been convicted, or found not guilty by reason of insanity of any of these offenses in the 10 years preceding the date of this application. A conviction means any finding of guilt, plea of guilty, or plea of *nolo contendere*.
I understand that if I am convicted or found not guilty by reason of insanity of any of the crimes listed above in the future, I must report such a conviction or finding of not guilty by reason of insanity to the Airport Security Coordinator within 24 hours.

By checking this box, I acknowledge and disclose to the Airport Security Coordinator that I have been convicted of one of these crimes in the 10 years preceding the date of this application. I understand that by failing to disclose this information it can lead to disqualification for an airport badge and fines by TSA.

(Signature and Date)

Section III – Applicants Security Responsibility Agreement

1. I will not allow anyone else to use my ID badge or access media.
2. I will wear my ID badge on my outermost garment, waist or above at all times when in the SIDA or sterile areas.
3. I will challenge all individuals I encounter to ensure that the airport issued ID media is valid. I will report those who are not displaying an ID badge in a SIDA area to the Security Office or LEO.
4. I will ensure proper closing, locking, and securing of any access point I use.
5. I will not allow anyone to follow me (piggyback) through any Secured Area door. When going through an AOA access gate with my vehicle I will follow AOA escort procedure.
6. I will report immediately if either my airport issued ID or access media is lost or stolen to the Security Department or Airport LEO.
7. If I am granted escort privileges, I fully understand I am responsible for the control of the person(s) I am escorting and that I understand the escort procedures and the reporting of unusual activity to the Security Department or Airport LEO.
8. I will report immediately any security violation I witness to the Security Department or Airport LEO.
9. I fully understand that pursuant to 49 USC §44903, any person and his/her accessible property accessing the Secured Area, AOA, or Sterile Area of the airport are subject to search by TSA or other authorized officials.
10. I understand the consequences for unauthorized disclosure (civil penalty action that may include fines) of Sensitive Security Information material. (See Section 1520.17 of Title 49 of the United States Code).

I have read the above security procedures and I understand that the failure to comply with any of them may result in the revocation of my ID badge or access media, which means I will not be allowed access to the security controlled areas of the airport, furthermore, I may be subject to civil penalty action from the Transportation Security Administration.

The information that 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 on this application can be punished by fine or imprisonment or both. (See Section 1001 of Title 18 of the United States Code).

Signature

Date

Section IV – Criminal History Record Check (CHRC) Certification

Name of Company _____

I certify that an FBI CHRC has been conducted for _____ on
(Applicants Name)

_____ in accordance with CFR 1542.209. The fingerprint Case No. is _____
(Date)

Certification Officials Name _____ Title _____

Certification Officials Signature _____ Date _____

Section V - SOCIAL SECURITY NUMBER CERTIFICATION

"I authorize the Social Security Administration to release my Social Security Number and full name to the Transportation Security Administration, Enrollment Services and Vetting Program, 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.

Signature: _____ Date of Birth: _____

SSN and Full Name: _____

Section VI – Authorized Signatory Certification

I attest, as an authorized Signatory, that all information contained herein is true, and that the applicant is currently employed and does so require unescorted access authority to the areas checked below. The individual applicant acknowledges their security responsibilities under 49 CFR 1540.105(a). If I submit an air carrier case number and date or as a condition of employment with a federal, state or local government I certify in accordance with the TSR 1542.209 and 1544.229, we have conducted the appropriate Fingerprint based Criminal History Records Check required to grant unescorted access to this individual and have determined that this individual meets all the requirements of the regulations and there were no disqualifying offenses. This individual is eligible for a badge permitting unescorted access pending airport approval. If this applicant no longer requires unescorted access to any or all areas of the airport, I will immediately notify the SYR Airport Security Coordinator.

- Reason for Application?** **New** **Renewal** **Lost/Stolen**
 Secured Area Privileges **AOA** **Sterile** **Request Escort Privileges** **Request Driving Privileges**

Authorized Signatory (Please Print)

Authorized Signatory Signature (Application Valid for 30 Days after Signed)

Date

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.

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.

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.

