



**Privacy Impact Assessment Update
for the
Airmen Certificate Vetting Program**

DHS/TSA/PIA-011(a)

September 20, 2016

Contact Point

Jason Hull

Aviation Programs Branch

Office of Intelligence and Analysis

Transportation Security Administrator

Jason.Hull@tsa.dhs.gov

Reviewing Official

Jonathan R. Cantor

Acting Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The Department of Homeland Security (DHS) Transportation Security Administration (TSA) conducts security threat assessments (STA) on Federal Aviation Administration (FAA) Airmen Certificate applicants and holders to ensure that the individual does not pose or is not suspected of posing a security threat. This Privacy Impact Assessment (PIA) update reflects the FAA's final rule that would expand this population to include operators of Small Unmanned Aircraft Systems for non-hobby and non-recreational purposes who will be issued remote pilot certificates, a type of Airmen Certificate.

Overview

The TSA conducts an STA to determine whether an Airmen Certificate holder or applicant poses or is suspected of posing a security threat. Security threat has been defined as a threat to transportation or national security, a risk of air piracy or terrorism, a threat to airline or passenger safety, or threat to civil aviation security.¹

The FAA has issued a Final Rule² on proposed operating and certification requirements to allow small unmanned aircraft systems (UAS) to operate for non-hobby and non-recreational purposes. A small UAS consists of a small unmanned aircraft (which, as defined by statute, is an unmanned aircraft weighing less than 55 pounds) and equipment necessary for the safe and efficient operation of that aircraft. The FAA has accommodated non-recreational small UAS use through various mechanisms, such as special airworthiness certificates, exemptions, and certificates of waiver or authorization. Under the Final Rule, the FAA will collect and forward information from operators to TSA for a security threat assessment. Once TSA notifies the FAA that the individual does not pose a security threat, the FAA will issue a temporary certificate, and then a final certificate once FAA internal procedures are complete. If TSA determines that an airman certificate applicant poses a security risk, 49 U.S.C. 46111 requires the FAA to deny the application for a certificate or amend, modify, suspend, or revoke (as appropriate) any part of an airman certificate based on TSA's security findings. Applicants who already hold a Pilot's Certificate under 14 CFR Part 61 will be issued a temporary certificate immediately upon acceptance of their application because they already undergo a TSA STA.

Airmen Certificates do not expire and all Airmen Certificate holders will be recurrently vetted.

¹ 49 USC 46111; 49 CFR 1540.115, 1540.117.

² http://www.faa.gov/uas/media/RIN_2120-AJ60_Clean_Signed.pdf



Reason for the PIA Update

This PIA update reflects that TSA will conduct STAs on a new category of Airmen Certificate, issued by the FAA. The new rule adopts specific requirements and procedures for the operation of small UAS in the National Airspace System for non-hobby or non-recreational purposes. Under the rule, the person who manipulates the flight controls of a small UAS would be defined as an operator, and, in most cases, would be subject to a TSA STA.

This update also reflects the following updates to the PIA published in 2007: (1) TSA does not perform recurrent immigration or criminal record checks on Airmen Certificate holders, but may consider these factors as part of its assessment of security threat if it learns of applicable derogatory information; (2) the FAA permits a web-based application from its Airmen Certificate applicants, as well as paper-based means; and (3) finally, this PIA update reflects a change to the zip code for the TSA Freedom of Information Act (FOIA) office to: FOIA Officer, Transportation Security Administration, TSA-20, Arlington, VA 20598-6020.

Privacy Impact Analysis

Authorities and Other Requirements

The authorities listed in the October 22, 2007 PIA continue to apply to the vetting of Airman Certificates. FAA issued a Final Rule,³ which makes operators of small UAS subject to TSA STA.

Characterization of the Information

TSA continues to collect the same information as described in the original PIA. The FAA will now also provide to TSA status information of an airman. This information, which would typically be maintained as a historical record of certification, includes: unique Airmen identification number, certificate type, and certificate class(es).

Uses of the Information

No changes. TSA will continue to use this information to carry out STAs to ensure that Airmen Certificate holders or applicants do not pose a threat to transportation or national security. The STA includes checking the individual's information against terrorist-related, criminal, and immigration databases that TSA maintains or uses.

³ http://www.faa.gov/uas/media/RIN_2120-AJ60_Clean_Signed.pdf



The Social Security number (SSN) is collected to prevent misidentifying persons who may have the same name or other identifiers on the watch lists or other lists.

Notice Requirements

No changes. FAA provides a Privacy Act statement on the application. In the event that an individual is determined to be a security threat and the individual believes that the results of the screening are inaccurate, he or she will be informed by TSA on how to pursue redress. The FAA System of Records Notice (SORN)⁴ provides notice to individuals regarding the collection of information.

Individuals also have an opportunity and right to decline to provide their information during the application process and during any redress.

The individual does not have the right to consent to particular uses of the information provided as TSA determines whether the individual poses or is suspected of posing a security threat. All uses of such information by TSA will be consistent with the Privacy Act and the applicable system of records notice, DHS/TSA-002 Transportation Security Threat Assessment System.⁵

Data Retention by the Project

No changes. TSA will continue to retain data it receives from FAA concerning the STAs conducted in accordance with record schedules approved by the National Archives and Records Administration (NARA). As Airmen Certificates have no expiration dates, an individual's valid certificate record, either active or non-active, will be retained unless TSA receives notification that the record is no longer valid.

TSA will destroy records one year after an individual's access is no longer valid. For individuals that may originally have appeared to be a match on a watch list, but are subsequently cleared, TSA will retain the records for at least seven years, or one year after the individual's certificate is no longer valid. For individuals who are an actual match to a watch list or otherwise determined to pose a threat to transportation or national security, TSA will retain the records for ninety-nine years, or seven years after TSA learns that the individual is deceased, whichever is shorter.

⁴ DOT/FAA 847 Aviation Records on Individuals, 75 FR 68849 (November 9, 2010).

⁵ DHS/TSA-002 Transportation Security Threat Assessment System, 79 FR 46862 (August 11, 2014).



Internal and External Information Sharing

No changes. Internally, TSA will continue to share the information collected on Airmen Certificate holders and applicants as well as STA information with DHS employees and contractors who have a need for the information in the performance of their duties. In the ordinary course, this involves personnel within the Office of Intelligence & Analysis (OIA) and the Office of Law Enforcement involved in the STA process.

Externally TSA will continue to share information, such as results of STAs, with the FAA. TSA may also share biographic information about individuals posing, or suspected of posing, a security threat with the Terrorist Screening Center (TSC). TSA may share additional information with other federal, state, tribal, territorial, or local law enforcement or intelligence agencies in accordance with the official, routine uses identified in the applicable Privacy Act SORN, DHS/TSA-002 Transportation Security Threat Assessment System.

Redress

TSA updated the address for mailing Freedom of Information Act (FOIA) or Privacy Act (PA) requests. Individuals wishing to access his or her information may submit a FOIA/PA request to TSA in writing by mail to:

FOIA Officer
Transportation Security Administration, TSA-20
Arlington, VA 20598-6020.

If TSA determines that an Airmen Certificate holder or applicant poses, or is suspected of posing, a threat to transportation or national security, TSA will send the individual an Initial Determination of Threat Assessment (IDTA). U.S. Citizens, Lawful Permanent Residents, and Aliens will have an opportunity to seek redress on the basis that they have been misidentified or that the underlying information pertaining to them is erroneous.



Auditing and Accountability

No changes. TSA systems for STAs maintain an auditing function of individuals who access the system.

Responsible Official

Jason Hull
Aviation Programs Branch
Office of Intelligence and Analysis
Transportation Security Administrator
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security