Department of Homeland Security
Office of Inspector General

Transportation Security Administration (TSA) Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures

Homeland Security

July 7, 2011

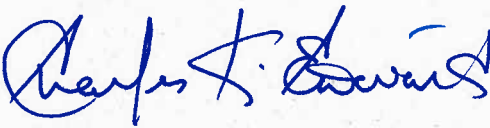|	
MEMORANDUM FOR:	John S. Pistole Administrator Transportation Security Administration
FROM:	Charles K. Edwards Acting Inspector General
SUBJECT:	*Final Letter Report: Transportation Security Administration (TSA) Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures* *OIG Report No. OIG-11-96*

Attached for your information is our final letter report, *Transportation Security Administration (TSA) Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures.* TSA did not provide formal comments to the report.

Consistent with our responsibility under the *Inspector General Act*, we are providing copies of our report to appropriate congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Should you have any questions, please call me, or your staff may contact Carlton I. Mann, Assistant Inspector General for Inspections, at (202) 254-4205.

Attachment

Background

The *Federal Aviation Act of 1958*, as amended, allows the Administrator of the Federal Aviation Administration (FAA) to issue an airmen certificate to several categories of aviation-related employees.[1] Those categories of aviation workers include commercial, private, student, sport, recreational, airline transport, and foreign pilots; flight and ground instructors; control tower operators; flight navigators, engineers and attendants; aircraft mechanics and repairmen; and parachute riggers. FAA requires applicants for these certificates to submit biographic and other information on an application form, including whether they have completed the necessary prelicensing training; whether they have been recommended by an examiner or instructor; and, if foreign-licensed, which country issued the license.

The *Aviation and Transportation Security Act* requires that the Transportation Security Administration (TSA) assess information in order to identify individuals who pose a threat to transportation security and coordinate countermeasures with other federal agencies, including FAA.[2] The *Aviation and Transportation Security Act* also requires TSA to work with FAA to take actions that may improve aviation safety or air carrier operations.[3] In addition, the *Intelligence Reform and Terrorism Protection Act of 2004* requires TSA to screen individuals against all appropriate records before FAA issues an airman certificate.[4] If TSA determines that an individual holding an airman certificate poses a security threat, TSA may recommend that FAA immediately suspend and ultimately revoke the certificate.

As part of its compliance with the *Aviation and Transportation Security Act*, FAA currently provides TSA with data from the Airmen Registry database daily. The data include biographic information on all airman certificate holders. In early 2009, TSA performed a biographic name-based security threat assessment for every individual airman certificate issued by FAA. The name-based security threat assessment consisted of matching FAA biographic data, including variations, against the Terrorist Screening Database (TSDB) to determine whether credible information indicated that the individual holding a certificate is involved, or suspected of being involved, in any activity that could pose a threat to transportation or national security. TSA analysts manually review potential matches identified by the automated matching process and, if necessary, refer potential matches to TSA's Threat Assessment and Credentialing Office (TTAC) for investigation. For example, if a name matches a TSDB record but the date of birth and other indicators are different, the analyst might recommend that FAA approve the individual for an airman certificate without further investigation. Conversely, if the name and other indicators match the information on the watch list, the analyst would refer the potential match to TTAC for investigation. The more thorough investigation includes coordinating information from TSA, FAA, and additional intelligence and law

---

[1] 49 U.S.C. § 44703(a).
[2] 49 U.S.C. § 114(f).
[3] 49 U.S.C. § 114(f)(13).
[4] 49 U.S.C. § 44903(j)(2)(D)(i).

enforcement agencies to determine what kind of derogatory information exists for the individual. TSA also coordinates with the National Counterterrorism Center (NCTC), Terrorist Screening Center, Terrorist Screening Operations Unit, Federal Bureau of Investigation (FBI), and Joint Terrorism Task Force to review relevant intelligence and make a determination regarding the airman certificate. Based on the results of this investigation, TSA determines whether the airman certificate should be revoked or suspended for a domestic applicant, or withheld for a foreign applicant.

In 2007, FAA and TSA signed an interagency agreement establishing a continuous vetting process for all new and existing airman applicants and certificate holders, valid for 10 years. TSA subsequently revetted all airman certificates issued through October 2009. Since then, TSA has vetted both new FAA airman certificate applicants and holders on an ongoing basis. New applicants are vetted against the TSDB and new TSDB records are matched against current certificate holders to determine if new derogatory information exists.[5]

Results of Review

As of February 2010, TSA had vetted approximately 4 million individuals who hold FAA airman certificates. These individuals have been vetted a total of nearly 6.8 million times against the TSDB, including the No Fly and Selectee subset lists. The TSDB is the U.S. government's consolidated watch list of all known or appropriately suspected terrorists. Among other things, TSA uses the No Fly and Selectee lists to identify individuals who are prohibited from boarding an aircraft or who are to receive additional physical screening before boarding aircraft. There are more FAA airman certificates than certificate holders because some individuals hold multiple certificates. For example, someone with a flight instructor's certificate would also hold a pilot's certificate. In addition, because FAA does not purge its files of inactive certificates, only approximately 1.3 million individuals hold active airman certificates.

The vetting process identified about 29,000 certificates that matched names in the TSDB. TSA analysts administratively determined that about 28,500 of these matches were invalid, so they did not refer them for a security threat investigation. TSA performed a security threat investigation on the remaining 506 that were determined to be true matches and recommended that 27 airman certificates be revoked.

---

[5] TSA said that it also matches airman certificate records against other name-based databases, and neither TSA nor FAA has the authority to conduct the FBI's Interstate Identification Index criminal history checks.

Inconsistencies Exist in Airman Data, and the Validation Process Can Be Enhanced

TSA's ability to vet airman records properly and thoroughly is limited by the quality of the biographic information (e.g., name and date of birth) in the FAA Airmen Registry and the databases against which the data are matched. Because FAA does not require unique identifiers, such as a Social Security number, TSA may not identify U.S. citizens who have provided false biographic information to receive an airman certificate.

FAA Social Security Number Data Are Incomplete and Inaccurate

Nearly 550,000 of about 1.3 million individuals on the Airmen Registry who have active certificates did not list a Social Security number that meets the Social Security Administration's (SSA) minimum requirements. However, currently FAA is not legally able to collect the Social Security numbers of Airmen Registry applicants because of *Privacy Act* restrictions. Specifically, Section 7 of the *Privacy Act* (5 U.S.C. § 552a note (Disclosure of Social Security Number)) provides that it shall be unlawful for any federal, state, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his Social Security number, unless the disclosure is required by federal statute.[6] Furthermore, the same section requires any such agency that requests an individual to disclose his Social Security number to inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Currently, *Privacy Act* forms given to applicants to the Airmen Registry state that disclosure of the Social Security number is voluntary. Therefore, although the FAA Airmen Registry application form provides space for the applicant to provide his or her Social Security number, FAA does not require applicants to provide it. When an applicant does not enter a Social Security number, a control number is automatically created.

Of the nearly 750,000 active airman records that contain a potentially valid Social Security number, more than 15,000 records do not match SSA's name, Social Security number, gender, or date of birth records. In more than 8,000 additional records, the name, Social Security number, gender, and date of birth match SSA's records; however, SSA indicates that those individuals are deceased. If FAA does not collect and validate Social Security number information for all applicable registrants, it is easier for individuals to create false identities by using fictitious biographic information.

TSA Vets FAA Records Against Subsets of Larger Terrorism and Criminal Databases

TSA does not vet airman certificate records against all criminal information. For example, the FBI does not receive all outstanding international warrants, arrests, and

---

[6] Another exception is if collection is pursuant to a system of records in existence before January 1, 1975, and disclosure was required prior to such date to verify an individual's identity.

convictions, although it receives some conviction information from international law enforcement organizations such as Interpol. As a result, some individuals who have active Airmen Registry certificates also have outstanding warrants or are known fugitives, as in the following examples:

- An individual with an active commercial pilot's certificate was indicted under the *Drug Kingpin Act of 1999* and is serving 20 years in a foreign prison.
- An individual with an active private pilot's certificate was indicted by federal authorities for arson and has fled the country.
- An individual with an active commercial pilot's license was charged with using laundered money to purchase airplanes to smuggle narcotics.

Although the FAA order on compliance and enforcement allows the FAA Administrator to issue an immediate order suspending or revoking a license in an emergency, emergency action of suspension or revocation will not be taken when the certificate holder is unable to exercise the privileges of the certificate, such as when he or she is in prison. In that case, FAA will issue a notice proposing certificate action instead of an emergency action, and suspension or revocation of the certificate will be decided by FAA counsel, generally within 30 days.[7] However, U.S. law requires FAA to revoke the certificate of any airman convicted of violating certain federal or state statutes involving controlled substances in conjunction with an airplane when the airman served as an airman or was aboard the aircraft in connection with the offense.[8] Even when there has been no conviction, FAA must revoke the license of an airman who knowingly carries out an activity punishable under these criminal statutes. Furthermore, FAA must amend, modify, suspend, or revoke a certificate if TSA notifies FAA that the holder poses, or is suspected of posing, a risk of air piracy or terrorism or poses a threat to airline or passenger safety.[9]

Security and Access Procedures Are Different at Commercial and General Aviation Airports

Airman certificates are not used to determine security and access at either commercial or general aviation airports. At commercial airports, Security Identification Display Area (SIDA) badges are the primary credential used to determine access to air operations area such as runways, tarmacs, maintenance facilities, and other secure facilities. General aviation airports are subject to fewer security regulations, but may institute their own security programs to limit access to the secure areas.[10]

---

[7] FAA Order 2150.3B, FAA Compliance and Enforcement Program, effective October 1, 2007.
[8] 49 U.S.C. § 44710.
[9] 49 U.S.C. § 46111.
[10] On October 30, 2008, TSA proposed new rules for large aircraft that would apply at general aviation airports. However, these rules have not yet been implemented.

Security and Access Procedures at Commercial Airports

At commercial airports, TSA is required to perform a Security Threat Assessment of all individuals who apply for airport-specific SIDA badges before the badge is issued. The assessment includes matches against the TSDB in an effort to determine whether the individual applying for the badge matches terrorism information. The assessment also matches biographic information from the applicant against the Systematic Alien Verification for Employment database to determine whether the applicant is legally permitted to work in the United States. In addition to these automated checks, airport security managers and air operators are required to perform a criminal history background check to determine whether the applicant has a disqualifying criminal history to preclude access to an airport's secured areas.

Commercial airports also restrict access to secured areas by using perimeter fencing as well as secured doors and checkpoints. Many checkpoints at commercial airports incorporate magnetometers or enhanced body imaging equipment to screen individuals.

Security and Access Procedures at General Aviation Airports

General aviation encompasses a wide range of activities, such as pilot training, business and personal charter flights, emergency medical services, and sightseeing. Operations at the Nation's 19,000 general aviation airports and helipads, only about a third of which are available for public use, range from short-distance flights in single-engine light aircraft to long-distance international flights in privately owned jets, and from emergency aero-medical helicopter operations to airship displays at sporting events. The sole common characteristic of general aviation operations is that flights are on demand, rather than routinely scheduled.

Airman certificates were not required or checked before an individual is granted access to air operations areas at the general aviation airports we visited. In addition, TSA officials told us TSA does not have the authority to issue security regulations for general aviation airports except for facilities located within Washington, DC, Metropolitan Area Flight Restricted Zone, roughly a 15-mile circle around Ronald Reagan Washington National Airport (Reagan National). Although TSA has published the *Security Guidelines for General Aviation Airports* that contain federally endorsed security procedures, the primary providers of aviation services at most general aviation airports are not subject to federal security regulations, and TSA's *Security Guidelines* are not mandatory.[11] For example, TSA recommends that "the identity of an individual renting an aircraft should be verified by checking an individual's government-issued photo identification, as well as his or her airmen's and current medical certificates." However, the general aviation operators at two major general aviation airports and one smaller general aviation airport near large East Coast metropolitan areas told us they do not require an individual to

---

[11] In written technical comments on this report, TSA also noted that standard security protocols for all 19,000 general aviation airports may be unfeasible given their range of sizes, locations, and operational capabilities.

provide either a government-issued identification or a valid airman certificate to board or fly a privately owned plane. General aviation operations personnel at those airports told us that a corporate pilot, for example, would be required only to show corporate identification to access the air operations area.

Some general aviation facilities restrict access to the air operations area with fencing or by monitoring doors, gates, and other entry points. However, access limitations procedures are not required. For example, we visited two general aviation airports in close proximity to each other in a large metropolitan area. While the first airport has a fenced perimeter, and a pilot or passenger is either physically escorted to an aircraft or physically observed until reaching an aircraft after entering the air operations area, the second airport does not a have a fence that encompasses the entire perimeter of the airport. Thus, at the second airport, unauthorized access to planes on the tarmac without the approval of an airport official can occur.

Additional Security Requirements for Direct General Aviation Access to Reagan National Airport

After discussions with other Department of Homeland Security components, the Department of Defense, and other federal agencies, TSA issued an interim final rule in 2005 that amended and added aviation security regulations allowing general aviation operations at Reagan National to resume after the restrictions imposed post-September 11, 2001.[12] Taking into consideration the special security needs of Reagan National, the regulations require operators to comply with specific security procedures. FAA operational procedures allow 48 general aviation flights per day in and out of Reagan National. All general aviation flights must meet the security measures set forth in the Washington Reagan National Airport Access Standard Security Program. To meet security measures, TSA must complete a series of steps that include an inspection of crew, passengers, accessible and checked property, and the aircraft. Passenger and crew manifests must be submitted 24 hours in advance of each flight. TSA must execute name-based security threat assessments for all crewmembers and passengers and fingerprint-based criminal history records check for crewmembers. An armed security officer must be onboard each flight unless a Federal Air Marshal is onboard or the aircraft is flying to or from Reagan National without passengers. All Washington Reagan National Airport Access Standard Security Program flights must depart from an approved gateway location (a Fixed Base Operator that has been approved by TSA as a last point of departure for flights into Reagan National). According to TSA, there are 57 approved gateway locations.

---

[12] Ronald Reagan Washington National Airport: Enhanced Security Procedures for Certain Operations; Interim Final Rule. 49 C.F.R. Parts 1520, 1540, and 1562 (70 FR 41586; July 19, 2005).

Appendix A
Purpose, Scope, and Methodology

The Chairman and Ranking Member of the Senate Committee on Commerce, Science, and Transportation, and the Chairman and Ranking Member of its Subcommittee on Aviation Operations, Safety, and Security requested that we review current TSA vetting procedures for registrants applying for airman certificates, as well as access and security procedures at civilian general aviation airports. They specifically requested that we review TSA and general aviation airport procedures to determine (1) how TSA currently vets FAA airman certificate applicants, (2) whether there is evidence that current vetting procedures can be enhanced, and (3) what security procedures are in place to restrict access at civilian general aviation airports.

To determine how TSA vets FAA airman certificate applicants, we interviewed FAA and TSA personnel, reviewed vetting agreements between FAA and TSA, and reviewed vetting procedure documents and standards at TSA.

To determine whether there is evidence that vetting procedures can be enhanced, we requested all TSA data for the FAA Airmen Registry and matched the data against the SSA database to determine the extent to which TSA records could be validated against SSA data.

To determine what security procedures exist to restrict access at civilian general aviation airports, we visited several general aviation airports. We also interviewed TSA, FAA, and general aviation service providers about standard access and security procedures at general aviation airports.

We briefed TSA concerning the results of fieldwork and the information summarized in this report.

We conducted this performance audit between February and December 2010 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

We appreciate the efforts by TSA management and staff to provide the information and access necessary to accomplish this review.

Appendix B
Managements Comments to the Draft Letter Report

TSA did not provide formal management comments to the draft letter report.

Appendix C
Major Contributors to this Report

John Kelly, Director
Scott Wrightson, Audit Manager
Joshua Wilshere, Auditor

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Administrator, Transportation Security Administration
Director, TSA's GAO/OIG Audit Liaison Office
Director of Local Affairs, Office of Intergovernmental Affairs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Senate Committee on Homeland Security and Governmental
Affairs,
Senate Committee on Appropriations
House Committee on Homeland Security
House Committee on Appropriations

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

• Call our Hotline at 1-800-323-8603;

• Fax the complaint directly to us at (202) 254-4292;

• Email us at DHSOIGHOTLINE@dhs.gov; or

• Write to us at:
    DHS Office of Inspector General/MAIL STOP 2600,
    Attention: Office of Investigations - Hotline,
    245 Murray Drive, SW, Building 410,
    Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.