OFFICE OF INSPECTOR GENERAL

Testimony of Inspector General John Roth

Before the Subcommittee on Transportation and Public Assets, Committee on Oversight & Government Reform U.S. House of Representatives

"Securing Our Skies: Oversight of Aviation Credentials"

Homeland Security

February 3, 2016
1:00 PM

DHS OIG HIGHLIGHTS

Securing Our Skies: Oversight of Aviation Credentials

February 3, 2016

Why We Did This Audit

We conducted this review to identify enhancements to the Transportation Security Administration's (TSA) vetting of workers with access to secure areas of commercial airports for links to terrorism, criminal history, and lawful status. We also assessed the accuracy and reliability of data TSA uses for vetting.

What We Recommend

TSA should request and review additional watchlist data, require that airports improve verification of applicants' right to work, revoke credentials when the right to work expires, and improve the quality of vetting data.

For Further Information:
Contact our Office of Legislative Affairs at (202) 254-4100, or email us at DHS-OIG.OfficeLegislativeAffairs@oig.dhs.gov

What We Found

TSA's multi-layered process to vet aviation workers for potential links to terrorism was generally effective. In addition to initially vetting every application for new credentials, TSA recurrently vetted aviation workers with access to secured areas of commercial airports every time the Consolidated Terrorist Watchlist was updated. However, our testing showed that TSA did not identify 73 individuals with terrorism-related category codes because TSA was not authorized to receive all terrorism-related information under the interagency watchlisting policy effective at the time of our audit.

TSA had less effective controls in place for ensuring that aviation workers 1) had not committed crimes that would disqualify them from having unescorted access to secure airport areas, and 2) had lawful status and were authorized to work in the United States. In general, TSA relied on airport operators to perform criminal history and work authorization checks, but had limited oversight over these commercial entities. Thus, TSA lacked assurance that it properly vetted all credential applicants.

Further, thousands of records used for vetting workers contained potentially incomplete or inaccurate data, such as an initial for a first name and missing social security numbers. TSA did not have appropriate edit checks in place to reject such records from vetting. Without complete and accurate information, TSA risks credentialing and providing unescorted access to secure airport areas for workers with potential to harm the nation's air transportation system.

TSA Response

TSA concurred with all six recommendations. As of the date of this testimony, three recommendations are closed and three are open and resolved, meaning that TSA and OIG have agreed on the corrective actions that TSA will take to close the recommendations.

Chairman Mica, Ranking Member Duckworth, and Members of the Subcommittee: thank you for inviting me here this afternoon to discuss the results of the Office of Inspector General's audit of the Transportation Security Administration's vetting of employees with access to secure areas of the airports.[1] We also reported on TSA worker vetting operations in 2011 and prior years.[2] In addition to reviewing vetting operations, in the past we have also used covert testing to determine whether unauthorized and potentially dangerous individuals could gain access to secured airport areas.[3]

TSA uses multiple layers of security to ensure the safety of the traveling public and transportation systems. Aviation worker vetting is just one area that we have reviewed; we have testified before this and other committees several times in the last year on multiple transportation security vulnerabilities that we believe TSA needs to address. Since 2004, we have published more than 120 audit and inspection reports about TSA's programs and operations. Our work includes evaluations of passenger and baggage screening, TSA PreCheck, TSA acquisitions, and TSA equipment deployment and maintenance.

In our most recent audit on aviation worker vetting, we generally found:

- TSA's layered controls for vetting workers for terrorism are generally effective. However, TSA did not identify 73 individuals with terrorism-related category codes because it was not authorized to receive all terrorism-related categories under current interagency watchlisting policy.
- TSA had less effective controls in place to ensure that airports have a robust verification process over a credential applicant's criminal history and authorization to work in the United States.
- TSA needs to improve the quality of data used for vetting purposes.

My testimony today will discuss each of these areas in further detail.

BACKGROUND ON TSA VETTING

TSA was created in 2001 to ensure the safety and free movement of people and commerce within the Nation's transportation systems. As part of this mission,

[1] *TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98
[2] *TSA's Oversight of the Airport Badging Process Needs Improvement*, OIG-11-95; *TSA Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures*, OIG-11-96; *Transportation Security Administration's Aviation Channeling Services Provider Project*, OIG-13-42; *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening*, OIG-09-05
[3] *Covert Testing of Access Controls to Secured Airport Areas, OIG-12-26*

TSA has statutory responsibility for properly vetting aviation workers such as baggage handlers and airline and vendor employees.

Federal regulations require individuals who apply for credentials to work in secure areas of commercial airports to undergo background checks. TSA and airport operators are required to perform these checks prior to granting individuals badges that allow them unescorted access to secure areas. Each background check includes:

- a security threat assessment from TSA, including a terrorism check;
- a fingerprint-based criminal history records check (CHRC); and
- evidence of the applicants' authorization to work in the United States.

Airports collect the information used for vetting, including each applicant's name, address, date of birth, place of birth, country of citizenship, passport number, and alien registration number (if applicable). TSA also relies on airport or air carrier employees to collect applicants' fingerprints for the CHRC.

Once it receives biographic data, TSA electronically matches credential applicants against its extract of the Government's Consolidated Terrorist Watchlist to identify individuals with potential links to terrorism. TSA also recurrently vets airport workers every time it receives a watchlist update. TSA identifies potential matches to terrorism-related information using varied pieces of data such as name, address, Social Security number (SSN), passport number, and alien registration number. TSA analysts manually review potential matches to determine whether cases represent a true match of an applicant to terrorism-related information and the risk posed by the case. Based on this review, TSA may direct the airport to grant, deny, or revoke a credential after coordination with other governmental organizations.

Airport operators are responsible for reviewing aviation worker criminal histories and his/her authorization to work in the United States. For the criminal history check, applicants submit fingerprint records through airport operators and TSA for transmittal to the FBI. TSA then receives the results of the fingerprint check and provides them to airport operators for review. Certain criminal offenses—such as espionage, terrorism, and some violent offenses and felonies—are disqualifying offenses that should prevent an individual from unescorted access to secured areas of an airport. TSA and the airports also conduct checks to verify an individual's immigration status and authorization to work, respectively.

RESULTS

Vetting for Terrorism Links

We found that TSA was generally effective in identifying individuals with links to terrorism. Since its inception in 2003, TSA has directed airports to deny or revoke 58 airport badges as a result of its vetting process for credential applicants and existing credential holders. In addition, TSA has implemented quality review processes for its scoring model, and has taken proactive steps based on non-obvious links to identify new terrorism suspects that it nominates to the watchlist.

Despite rigorous processes, TSA did not identify 73 individuals with links to terrorism because TSA is not cleared to receive all terrorism categories under current inter-agency watchlisting guidance.[4] At our request, the National Counterterrorism Center (NCTC) performed a data match of over 900,000 airport workers with access to secure areas against the NCTC's Terrorist Identities Datamart Environment (TIDE). As a result of this match, we identified 73 individuals with terrorism-related category codes who also had active credentials. According to TSA officials at the time of our report, current interagency policy prevented the agency from receiving all terrorism-related codes during vetting.

TSA officials recognized that not receiving these codes represents a weakness in its program, and informed us that TSA cannot guarantee that it can consistently identify all questionable individuals without receiving these categories. In 2014, the TSA Administrator authorized his staff to request some missing category codes for vetting. However, according to an official at the DHS Office of Policy, TSA needed to work with DHS to formalize a request to the Watchlisting Interagency Policy Committee in order to receive additional categories of terrorism-related records. Recently, TSA informed us that it has taken actions to address this issue. Since the issuance of our report, we have received documentation satisfying our office that TSA has taken corrective action to address this weakness.

Vetting for Criminal Histories

Airport operators review criminal histories for new applicants for badges to secure airport areas after receiving the results of FBI fingerprint checks through TSA but do not conduct recurrent criminal history vetting, except for the U.S. Marshals Service Wants and Warrants database. This is because

[4] The Interagency Policy Committee responsible for watchlist policy determines what terrorism-related categories are provided to TSA for vetting, while the DHS Watchlist Service provides allowable information to TSA.

aviation worker vetting is considered to be for non-criminal justice purposes. Instead, we found airports relied on individuals to self-report disqualifying crimes. As individuals could lose their job if they report the crimes, individuals had little incentive to do so.

TSA also did not have an adequate monitoring process in place to ensure that airport operators properly adjudicated credential applicants' criminal histories. While TSA facilitated the CHRC for aviation worker applicants, over 400 commercial airports maintained the ultimate authority to review and determine whether an individual's criminal history contained disqualifying crimes under Federal law. TSA officials informed us that airport officials rarely or almost never documented the results of their CHRC reviews electronically. Without sufficient documentation, TSA cannot systematically determine whether individuals with access to secured areas of the airports are free of disqualifying criminal events.

TSA has taken steps to address weaknesses in criminal history vetting. TSA has planned a pilot of the FBI's "Rap Back" program to receive automated updates from the FBI for new criminal history matches associated with airport workers so that the airports can take actions. Recently, TSA informed us that it plans to start this pilot program for multiple airports in February 2016.

Vetting for Authorizations to Work

We also found weaknesses in the verification process for an individual's authorization to work in the United States. Airport operators are required to ensure that aviation workers are authorized to work in the United States prior to sending their information to TSA for review. TSA then verifies that aviation workers have lawful status to be in the United States. However, our review of TSA data showed that TSA has had to send nearly 29,000 inquiries to credential applicants regarding their lawful status since program inception in 2004. Of those individuals, over 4,800 were eventually denied credentials because TSA determined that they did not prove lawful status even after appeal. This occurred despite the fact that these individuals had previously received clearance from the airports as being authorized to work.

Additionally, we found that TSA did not require airports to restrict the credentials of individuals who may only be able to work in the United States temporarily. Consequently, airports did not put expiration dates on the badges. Although airports are required to verify work authorizations upon badge renewal every 2 years, or whenever another credential is requested, individuals may continue to work even when they no longer have lawful status during the period between badge renewals. Without ensuring that an individual's credential is voided when he or she is no longer authorized to work, TSA runs

the risk of providing individuals access to secure airport areas even though they no longer have the authorization to work in the United States.

TSA's Office of Security Operations performed annual inspections of commercial airport security operations, including reviews of the documentation that aviation workers submitted when applying for credentials. However, due to workload at larger airports, this inspection process looked at as few as one percent of all aviation workers' applications. In addition, inspectors were generally given airport badging office files, which contained photocopies of aviation worker documents rather than the physical documents themselves. An official from this office told us that a duplicate of a document could hinder an inspector's ability to determine whether a document is real or fake, because a photocopy may not be matched to a face, and may not show the security elements contained in the identification document. Fortunately, as a result of our audit, TSA has taken corrective action and TSA inspectors will now be able to examine original documents during annual security inspections.

TSA Can Improve the Reliability of Its Vetting Data

TSA relied on airports to submit complete and accurate aviation worker application data for vetting. However, we identified thousands of aviation worker records that appeared to have incomplete or inaccurate biographic information as follows:

- 87,000 active aviation workers did not have SSNs listed even though TSA's data matching model identified SSNs as a strong matching element.
- 1,500 records in TSA's screening gateway had individuals' first names containing two or fewer characters.
- Over 300 name records contained a single character.
- An additional 75,000 records listed individuals with active aviation worker credentials as citizens of non-U.S. countries, but did not include passport numbers. Out of those records, over 14,000 also did not list alien registration numbers. According to TSA, the passport number is a desired field to collect, but is not required.

In addition to the data completeness issues that we identified, TSA independently determined that airports may not be providing all aliases used by applicants undergoing security threat assessments. This typically occurred when TSA's vetting process discovered that individuals had used aliases. Complete and accurate aliases are important to the accuracy and effectiveness of TSA's vetting processes. TSA has directed airports to report all aliases; however, to the extent that airports do not ensure that aliases are captured

and provided to TSA, TSA terrorism vetting may be limited for certain individuals.

TSA has taken steps to address some of these weaknesses. TSA made system enhancements between 2012 and 2014 designed to improve the quality of data that it received from airports. For example, TSA will refuse to vet individuals if their birthdates show that they are younger than 14 or older than 105 and encourage airports to submit electronic copies of immigration paperwork with applications to expedite the vetting process. These enhancements were expected to become effective for new or reissued badges within 2 years of being implemented. Recently, TSA informed us that it has drafted additional data requirements that will become effective in the second quarter of FY 2016.

CURRENT STATUS OF RECOMMENDATIONS

We made six recommendations in our report. TSA agreed with all of our recommendations and provided target completion dates for corrective actions. To date, TSA has completed corrective actions to close three of our recommendations, and has reported actions underway to close the remaining three recommendations in the second quarter of FY 2016. TSA considers many details of its corrective actions to be Sensitive Security Information and we cannot include them here. In addition, TSA has performed its own review of the 73 individuals we identified with terrorism-related category codes and determined that none of the individuals represented a threat to transportation security. However, TSA's inability to have access to all terrorism-related information presents a risk to transportation security, and we are pleased that TSA has taken corrective actions in response to our audit recommendation that address that risk. Following is the current status of our six recommendations.

Table 1: Status of OIG Recommendations to Enhance TSA's Vetting of Aviation Workers

Recommendation	Current Status	Details
Follow up on the request for additional categories of terrorism-related records	CLOSED	Closed in January 2016. TSA considers details of its corrective actions to address this recommendation to be Sensitive Security Information.
Require inspectors to view original identity documents supporting airport adjudication of an applicant's criminal history and work authorization	CLOSED	TSA provided documentation in October 2015 that it had updated its Compliance Program Manual for Transportation Security Inspectors to comply with our recommendation.
Pilot FBI's Rap Back Program and take steps to institute recurrent vetting of criminal histories at all commercial airports	OPEN, RESOLVED	TSA reported in January 2016 that it projected the pilot program to begin in February 2016.
Require airports to link credential end dates to temporary work authorization end dates	CLOSED	TSA provided documentation in December 2015 to show it had posted additional guidance for airport operators to deactivate badges promptly when an individual's authorization to work ends.
Perform analysis to identify and address airports' weaknesses in determining applicants' lawful status	OPEN, RESOLVED	TSA reported in January 2016 that it was reviewing records and anticipated closure in the second quarter of FY 2016.
Implement data quality checks to ensure complete and accurate data as required by TSA policy	OPEN, RESOLVED	TSA reported in January 2016 that it had identified enhancements and anticipated closure in the second quarter of FY 2016.

Our office will continue to follow up on implementation of these corrective actions.

ONGOING REVIEWS

We have two additional ongoing reviews related to the TSA credentialing process. First, we are reviewing TSA's oversight of airport operators' accountability procedures for Secure Identification Display Area (SIDA) badges, which airport operators issue to airport and TSA employees who require access to secure areas. TSA oversees the implementation of airport operators' security programs, including the accountability procedures for SIDA badges and access

control systems. We are testing selected internal controls airport operators have in place to mitigate the potential risks of unaccounted for, lost, or stolen SIDA badges. OIG has tested selected internal controls at 24 of the largest U.S. airports and will issue a report on our findings later this year.

We are also reviewing the applicant screening process for Transportation Workers Identification Credential (TWIC) program to determine whether it is operating effectively and ensuring only eligible TWIC card holders remain in the program. We expect to complete this review this summer, but because of some of our preliminary findings, TSA has already begun assessing some program shortfalls.

CONCLUSION

TSA has the responsibility to ensure transportation security and the free and safe movement of people and commerce throughout the Nation. Effectively carrying out this responsibility is of paramount importance, given emerging threats and the complex and dynamic nature of this Nation's transportation system. We previously testified about major TSA deficiencies in accomplishing its transportation security mission, including extensive failures at TSA checkpoints identified during recent penetration testing, as well as weaknesses in its PreCheck vetting and screening process. With our recent report, we add another security vulnerability that TSA must address: ensuring it has all relevant terrorism-related information when it vets airport employees for access to secure airport areas. We will continue to monitor TSA's progress as it takes corrective actions to address these vulnerabilities.

COMPUTER MATCHING ACT EXCEPTION

I would be remiss if I did not mention the data matching issues that we encountered while conducting this audit. As part of this review, we collaborated with the NCTC to perform a data match of aviation worker's biographic data against TIDE to determine if TSA identified all individuals with potential links to terrorism. Because we do not have an exemption from the Computer Matching Act, it took us 18 months to get a Memorandum of Understanding in place with the NCTC in order to perform this data match – and that was with full cooperation from the NCTC.

We support pending legislation co-sponsored by the Chairman and Ranking Member of the full Committee, the *Inspector General Empowerment* Act (H.R. 2395), that would give Inspectors General a computer matching exception. This would enable us to conduct these types of audits on a more frequent basis and with greater ease. We are grateful that the legislation has been reported to the House by this Committee and are hopeful for continued legislative action this Congress.

Mr. Chairman, thank you for inviting me to testify here today. I look forward to discussing our work with you and the Members of the Subcommittee.

Appendix A
Reports Cited in Testimony

TSA Can Improve Aviation Worker Vetting (Redacted), OIG-15-98 (June 2015)

Transportation Security Administration's Aviation Channeling Services Provider Project, OIG-13-42 (February 2013)

TSA's Oversight of the Airport Badging Process Needs Improvement, OIG-11-95 (July 2011)

TSA Vetting of Airmen Certificates and General Aviation Airport Access and Security Procedures, OIG-11-96 (July 2011)

Covert Testing of Access Controls to Secured Airport Areas, OIG-12-26 (January 2012)

TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening , (OIG-09-05) (October 2008)

Appendix B
Current and Planned OIG Work on TSA

Projects In-Progress:

Project Topic	Objective
TSA Security Vetting of Passenger Rail Reservation Systems	Determine the extent to which TSA has policies, processes, and oversight measures to improve AMTRAK security.
Reliability of TWIC Background Check Process	Determine whether the screening process for the TWIC program is operating effectively and whether the program's processes ensure that only eligible TWIC card holders remain in the program.
TSA's Security Technology Integrated Program (STIP)	Determine whether TSA has incorporated adequate IT security controls for passenger and baggage screening STIP equipment to ensure it is performing as required.
TSA's Controls Over Access Media Badges	Identify and test selected controls over access media badges issued by airport operators.
TSA's Risk-Based Strategy	Determine the extent to which TSA's intelligence-driven, risk-based strategy informs security and resource decisions.
Airport Security Capping Report	Synthesize the results of our airport security evaluations into a capping report that recommends how TSA can systematically and proactively address these issues at airports nationwide.

Upcoming Projects:

Project Topic	Objective
Federal Air Marshal Service's Oversight of Civil Aviation Security	Determine whether the Federal Air Marshal Service adequately manages its resources to detect, deter, and defeat threats to the civil aviation system.
TSA Carry-On Baggage Penetration Testing	Determine the effectiveness of TSA's carry-on baggage screening technologies and checkpoint screener performance in identifying and resolving potential security threats at airport security checkpoints.
TSA's Classification Program	Determine whether TSA is effectively managing its classification program and its use of the Sensitive Security Information designation.
TSA's Office of Intelligence and Analysis	Determine whether TSA's Office of Intelligence and Analysis is effectively meeting its mission mandates.
Verification Review – *TSA's Screening of Passengers by Observation Techniques*	Conduct a verification review to ensure TSA has implemented our closed recommendations from our September 2013 report.