STATEMENT OF THE HONORABLE JOHN ROTH

INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON TRANSPORTATION SECURITY

U.S. HOUSE OF REPRESENTATIVES

CONCERNING

HOW TSA CAN IMPROVE AVIATION WORKER VETTING

JUNE 16, 2015

Chairman Katko, Ranking Member Rice, and Members of the Subcommittee: thank you for inviting me here today 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 recently on multiple transportation security vulnerabilities that we believe TSA needs to address. Since 2004, we have published more than 115 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 is 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, 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

---

[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; *Transportation Security Administration's Aviation Channeling Services Provider Project, OIG-13-42*

[3] *Covert Testing of Access Controls to Secured Airport Areas, OIG-12-26*

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 names, 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, current interagency policy prevents the agency from receiving all terrorism-related codes during vetting.

TSA officials recognize 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 must work with DHS to formalize a request to the Watchlisting Interagency Policy Committee in order to receive additional categories of terrorism-related records.

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. However, under current law and FBI policy, TSA and the airports are not legally authorized to conduct recurrent criminal history vetting, except for the U.S. Marshals Service Wants and Warrants database. This is because 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

[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.

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. TSA is planning this pilot program for multiple airports in late 2015.

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 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.

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. Pursuant to the *Privacy Act*, TSA is not authorized to require the collection of SSNs.
- 1,500 records in TSA's screening gateway had individuals' first names containing two or fewer characters.
- Over 300 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 were 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 will become effective for new or reissued badges, which should happen within 2 years as required by TSA's security policy.

RECOMMENDATIONS

We made six recommendations in our report:

- Follow up on the request for additional categories of terrorism-related records.

- Require inspectors to view original identity documents supporting airport adjudication of an applicant's criminal history and work authorization.
- Pilot FBI's Rap Back Program and take steps to institute recurrent vetting of criminal histories at all commercial airports.
- Require airports to link credential end dates to temporary work authorization end dates.
- Perform analysis to identify airports with weaknesses related to applicants' lawful status.
- Implement data quality checks to ensure complete and accurate data as required by TSA policy.

TSA agreed to all recommendations and provided target completion dates for corrective actions. DHS will follow up on implementation of these corrective actions.

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 legislation pending in the House, 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.

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.