OFFICE OF INSPECTOR GENERAL

TSA Can Improve Aviation Worker Vetting (Redacted)

Homeland Security

OIG-15-98

June 4, 2015

DHS OIG HIGHLIGHTS

TSA Can Improve Aviation Worker Vetting

June 4, 2015

Why We Did This

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 Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@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 is not authorized to receive all terrorism-related information under current interagency watchlisting policy.

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 airports 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.

Table of Contents

Appendixes

Abbreviations

CBP	Customs and Border Protection
CFR	Code of Federal Regulations
CHRC	Criminal History Records Check
CSG	Consolidated Screening Gateway
DAC	Designated Aviation Channeler
DHS	Department of Homeland Security
EAB	Encounter Analysis Branch
FBI	Federal Bureau of Investigation
IR&A	Investigations, Referrals & Analysis
NCTC	National Counterterrorism Center
OIG	Office of Inspector General
SAVE	Systematic Alien Verification for Entitlements Program
SIDA	Secure Identification Display Area
SSN	Social Security Number
TIDE	Terrorist Identities Datamart Environment
TSA	Transportation Security Administration
TVS	Transportation Vetting System
USCIS	United States Citizenship and Immigration Service
VAD	Vetting Analysis Division

Results of Audit

We reviewed the Transportation Security Administration's (TSA) controls over the vetting of aviation workers possessing or applying for credentials that allow unescorted access to secured areas of commercial airports. Specifically, we assessed TSA's process for vetting workers for terrorist links, criminal history, and lawful status. We also sought to determine the accuracy and reliability of data TSA uses for vetting.

We determined that TSA had multiple, layered controls for vetting workers for terrorism. TSA designed its vetting procedures to 1) match new applicants for credentials, and 2) repeatedly re-vet nearly 1 million existing credential holders against the Consolidated Terrorist Watchlist within minutes of receiving updated watchlist data. This process resulted in thousands of watchlist hits that TSA analysts manually reviewed during fiscal year 2014. TSA also proactively identified relationships between current credential holders and watchlisted individuals and nominated over 300 individuals to the watchlist across all credential programs. In addition, TSA recently made improvements to the quality of the aviation worker data used for vetting.

Despite these layered controls, our testing showed that TSA did not identify 73 individuals with terrorism-related category codes. According to TSA data, these individuals were employed by major airlines, airport vendors, and other employers. TSA did not identify these individuals through its vetting operations because it is not authorized to receive all terrorism-related categories under current interagency watchlisting policy. Excluded categories [redacted] TSA acknowledged that these individuals were cleared for access to secure airport areas despite representing a potential transportation security threat.

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 did not perform recurrent criminal records checks similar to its terrorism vetting due to current law and FBI policies. TSA depended on 467 commercial airports and air carriers to verify credential holders' criminal histories through a limited review process, and relied on the credential holders themselves to report disqualifying crimes to the airports where they worked. Further, TSA had to deny thousands of credentials to individuals because it could not verify their lawful status, even though airports represented that these individuals had passed the airports' own work authorization verification.

We identified thousands of TSA data records containing potentially incomplete and inaccurate biographic information. TSA relied on airports to gather complete and accurate information from the credential applicants. According to vetting officials, TSA can only vet workers based on data received from airports. While TSA had made some improvements to its data collection to meet its requirements, TSA lacked assurance that it properly vetted all credential applicants.

We recommended that TSA work with the necessary interagency partners to determine if its aviation worker credential program warrants the receipt of additional categories of terrorism-related data, require airports to improve their verification of applicants' right to work, and terminate credentials when the right to work expires. We also recommended that TSA take steps to ensure the data it uses for aviation worker vetting are complete and accurate.

Background

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 also has statutory responsibility for properly vetting aviation workers such as baggage handlers and airline and vendor employees with unescorted access to Secure Identification Display Area (SIDA) and sterile areas of commercial airports.

Chapter 49 of the Code of Federal Regulations (CFR) and TSA Security Directive 1542-04-08G require that individuals applying for credentials to work in secure areas of commercial airports undergo background checks prior to being granted badges that allow them unescorted access to secure areas. Each background check includes 1) a security threat assessment from TSA, including a terrorism check; 2) a fingerprint-based criminal history records check (CHRC); and 3) evidence of the applicants' right to work in the United States. The CHRC determines whether the credential applicant has a disqualifying criminal offense in the previous 10 years. These crimes fall into 28 categories, including crimes involving air safety as well as violent felonies, fraud, and bribery.

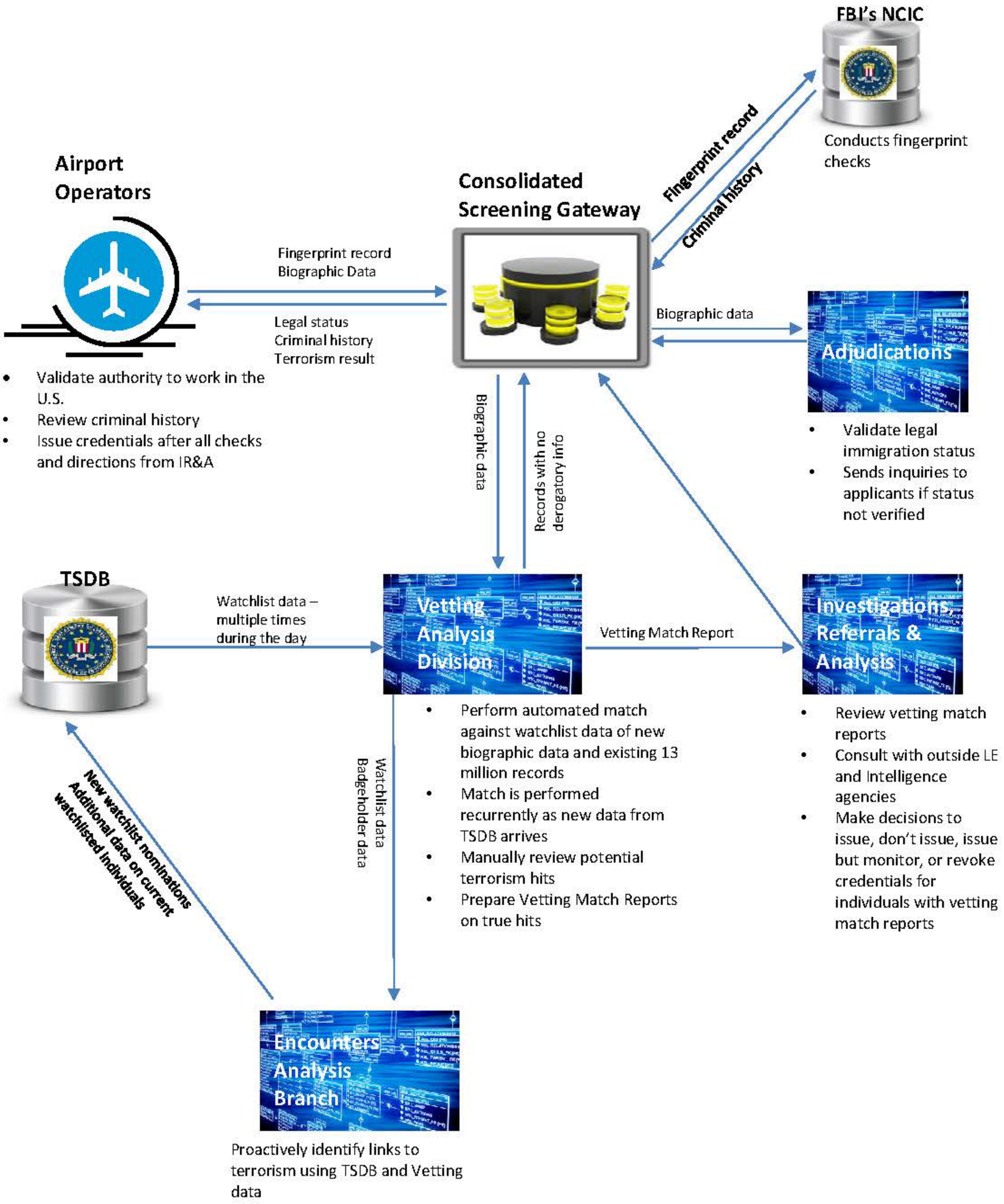
Under Security Directive 1542-04-08G, TSA relies on airport operators to collect and verify applicant data for individuals seeking credentials. This data includes each applicant's name, address, date of birth, place of birth, country of citizenship, passport number, and alien registration number (if applicable). Social security number (SSN) is not currently a required field on the aviation worker credential application, but is collected if provided by the applicant. TSA also relies on airport or air carrier employees to collect an applicant's fingerprints for the CHRC. Airports use one of three Designated Aviation Channelers (DAC) to submit prospective aviation worker information and changes to biographic data for existing workers to TSA. The DACs ensure the applicant's biographic and fingerprint information is complete and formatted properly before forwarding the information to TSA for vetting.

Once it receives biographic data from the Consolidated Screening Gateway (CSG), the Vetting Analysis Division (VAD) of TSA's Office of Intelligence and Analysis uses the Transportation Vetting System (TVS) to match credential applicants against its extract of the DHS Watchlist Service to identify individuals with potential links to terrorism. TSA also re-vets airport workers with unescorted access to secure areas of commercial airports against the watchlist on a recurring real-time basis. That is, it performs a match of all existing airport workers every time it receives watchlist updates, which may happen many times in a day.[1] TSA's matching model scores each worker it vets against the Consolidated Terrorist Watchlist using various rules, such as name matches; SSN, passport number or alien registration number matches; address matches; or combinations of different variables. TVS scores potential matches automatically and presents them to analysts for manual review and analysis. Analysts then determine whether the potential match represents a true name match. For true name matches, analysts prepare a preliminary vetting match report that includes all relevant information related to the match. VAD sends the report to TSA's Investigations, Referrals & Analysis (IR&A) to help conduct a full investigation.

Figure 1 provides an overview of this vetting process. As shown in figure 1, upon receiving information from VAD, the IR&A team performs additional research to determine whether a potential match is indeed a real match. If necessary, IR&A coordinates with other law enforcement or terrorism prevention agencies to arrive at a final disposition.

[1] In addition to aviation workers, TSA also recurrently re-vets over 13 million other credential holders in programs such as the Transportation Worker Identification Credential and Federal Aviation Administration Airmen Certificate.

Figure 1. TSA Vetting Process


FBI's NCIC
Conducts fingerprint checks
Airport Operators
Consolidated Screening Gateway
Fingerprint record
Criminal history
Fingerprint record
Biographic Data
Legal status
Criminal history
Terrorism result
Biographic data
Adjudications
Biographic data
Records with no derogatory info
TSDB
Watchlist data – multiple times during the day
Vetting Analysis Division
Vetting Match Report
Investigations, Referrals & Analysis
Watchlist data
Badgeholder data
New watchlist nominations
Additional data on current watchlisted individuals
Encounters Analysis Branch

Airport Operators:

- Validate authority to work in the U.S.
- Review criminal history
- Issue credentials after all checks and directions from IR&A

Adjudications:

- Validate legal immigration status
- Sends inquiries to applicants if status not verified

Vetting Analysis Division:

- Perform automated match against watchlist data of new biographic data and existing 13 million records
- Match is performed recurrently as new data from TSDB arrives
- Manually review potential terrorism hits
- Prepare Vetting Match Reports on true hits

Investigations, Referrals & Analysis:

- Review vetting match reports
- Consult with outside LE and Intelligence agencies
- Make decisions to issue, don't issue, issue but monitor, or revoke credentials for individuals with vetting match reports

Encounters Analysis Branch:

Proactively identify links to terrorism using TSDB and Vetting data

Source: Department of Homeland Security (DHS) Office of Inspector General (OIG) analysis of TSA vetting procedures.

Based on its additional research, IR&A may direct the airport to:

- grant the credential (for a new applicant),
- deny the credential (for a new applicant),
- revoke an existing credential (in the case of an existing credential holder who matched against the watchlist as part of the recurrent vetting process), or
- [redacted]

[redacted] IR&A confers with other governmental organizations, such as the Federal Bureau of Investigation (FBI), that have nominated an individual to the watchlist or may have an open case on the individual. In some instances, other governmental organizations may request that TSA not direct the airport to deny or revoke a credential because the denial or revocation may impact an open investigation.

[redacted]

TSA Security Directive 1542-04-08G requires airport operators to perform a CHRC for all employees who require unescorted access to SIDA and sterile areas of commercial airports, except for Federal, State, or local government employees who already have CHRCs performed as conditions of their employment. To perform the CHRC, applicants submit fingerprint records to the appropriate airport operators, who in turn provide the fingerprint records to TSA. TSA sends the fingerprint records to the FBI for a background check. FBI returns the results to airport operators through TSA. Airport operators are responsible for conducting reviews of the applicant's criminal history for criminal offenses that would disqualify the individual from unescorted access to secured areas of an airport. Disqualifying offenses are listed in 49 CFR 1542.209 and include espionage; sedition; treason; crimes involving terrorism, transportation security, or explosives; some violent offenses; and some felonies.

Chapter 49 of the CFR and TSA Security Directive 1542-04-08G require that prospective credential applicants undergo immigration checks to ensure that the individuals have lawful presence and that airport operators verify the applicant's authorization to work in the United States. This check occurs in two stages. First, airport operators collect and review documents validating that a credential applicant is authorized to work in the United States. For example, legal permanent residents and certain student visitors may have authorization to work in the United States, while tourists visiting the United States under a visitor visa would likely not have the right to work. The airport then forwards the validated file on the individual to TSA for a second review. During this review, TSA performs its verification to ensure that the individual has lawful status to be in the United States. According to TSA's Security Directive, airports have to verify an individual's authorization to work before sending their record to TSA for the security threat assessment, and not issue credentials unless the individual is authorized to work.

To check a prospective credential holder's lawful status, TSA's Security Threat Assessment Operations verifies against the U.S. Citizenship and Immigration Service's (USCIS) Systematic Alien Verification for Entitlements Program (SAVE) all individuals listed as being born outside the United States. SAVE provides the ability for Federal, State, or local benefit and licensing agencies to verify the immigration status of noncitizen applicants for Federal, State, or local benefits and licenses.

In 2011, we reported that TSA's oversight of commercial airports' badging process needed improvement, and made recommendations to TSA to help improve the accuracy and completeness of vetting information, improve identity verification, and require recurrent vetting of applicant criminal histories.[2] TSA took some steps to improve in those areas, including issuing guidance to airports to help improve data quality and encourage airport operators to use Customs and Border Protection's (CBP) Identification Verification guide for periodic training. However, TSA is not currently authorized under law and FBI policy to conduct recurrent criminal history records checks, although it has made efforts to gain the authorization to perform recurrent checks.

[2] DHS OIG, *TSA's Oversight of Airport Vetting Process Needs Improvement*, OIG-11-95, July 7, 2011.

TSA Can Enhance Its Process for Vetting Aviation Workers

TSA's multiple, layered controls for vetting potential and existing credential holders against the Consolidated Terrorist Watchlist were generally effective. TSA performed initial and recurrent vetting, regularly tested the algorithms it uses for vetting, and proactively identified new terrorism suspects for nomination to the watchlist. An independent match performed by the National Counterterrorism Center (NCTC) found that overall, the TSA algorithms used and the manual review process were effective in identifying prospective and existing credential holders' links to terrorism. However, we found that TSA did not receive certain terrorism-related category codes as part of the watchlist extract they used for vetting. Consequently, TSA's vetting process did not identify 73 aviation workers with active badges that we determined had terrorism-related category codes.

TSA had less effective controls in place for ensuring that airports vet aviation workers for disqualifying criminal records and authorization to work in the United States. TSA relied on airport operators to perform criminal history and work authorization checks and had limited access to documentation supporting the airports' credentialing decisions. As such, TSA lacked awareness of applicants' criminal histories. TSA also had to deny credentials to 4,800 individuals that the airports had previously cleared for work in the United States because it could not verify lawful status for those individuals.

TSA's Multi-Layered Process to Vet Workers for Links to Terrorism Was Generally Effective

The vetting and re-vetting procedures that TSA used were generally effective in identifying credential holders with links to terrorism. For example, 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. According to TSA's vetting managers, TSA's recurrent vetting process has been a crucial tool in ensuring the security of the Nation's transportation system. TSA has also taken the following steps to continually enhance this vetting process:

- TSA implemented a quality review process to test and refine the effectiveness of its scoring model. According to vetting officials, testing the scoring model allowed TSA to determine what percentage of potential matches would represent true name matches, and gave TSA the ability to optimize the number and type of matches it presented to analysts for manual review.

- The VAD tested its name matching algorithms against those of its peers. According to TSA officials, in 2013, TSA participated in a name-matching contest sponsored by the Mitre Corporation along with three other DHS name-matching systems from CBP and USCIS. TSA's TVS name-matching capabilities ranked first in the contest among DHS entrants based on an overall quality measure.

- In 2010, TSA created the Encounter Analysis Branch (EAB) team to leverage the vast amount of data it analyzed to proactively identify new terrorism suspects. For example, the EAB submits newly identified addresses, phone numbers, or other pertinent identifying information not currently included in a watchlist record. The EAB also submits new terrorist watchlist nominations, for example, if TSA determines there is sufficient information to link a credential holder to a known or suspected terrorist. According to TSA officials, for the 18-month period ending June 30, 2014, EAB analysis resulted in TSA submitting [redacted] terrorist watchlist nominations and providing new information for [redacted] records. In one example, TSA identified an aviation worker who [redacted] As a result of TSA's nomination, the aviation worker was added to the consolidated terrorist watchlist.

TSA Did Not Identify 73 Workers with Links to Terrorism

Although TSA's vetting procedures for terrorism were mostly effective, our testing determined that TSA did not identify 73 individuals with links to terrorism. This occurred because TSA is not authorized under current interagency watchlisting policy to receive certain terrorism-related category codes as part of the watchlist extract they used for vetting. TSA acknowledged that individuals in these categories represented a potential transportation security threat.

To assess the accuracy and effectiveness of TSA's terrorism vetting procedures, we asked NCTC to match over 900,000 records of active aviation workers against NCTC's Terrorist Identities Datamart Environment (TIDE).[3] Our analysis of NCTC results determined that TSA did not find 73 individuals linked to terrorism because the watchlist extract TSA received from the DHS Watchlist Service and used for vetting did not contain the terrorism codes associated with those individuals.[4] According to an official at the DHS Office of Policy, in order to receive additional categories of TIDE records, TSA must work with DHS to formalize a request to the Watchlisting Interagency Policy

[3] TSA maintains over 2 million aviation worker entities in the TVS vetting system. However, we did not submit all aviation worker records vetted by TSA to NCTC for matching. We eliminated inactive badge records that are retained by TSA, as well as badges for individuals who do not have access to secured areas of airports.

[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.

Committee through its Screening Coordination Office. Details on the individuals and their terrorism codes can be found in table 1.

Table 1: Categories of Aviation Worker Records with Terrorism Links

Terrorism-Related Category Code	Terrorism Record Category	Aviation Worker Record Matches
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	Total Records	73

Source: DHS OIG analysis of NCTC matching results.

As shown in table 1, codes TSA did not receive for vetting include [redacted] According to the DHS Screening Coordination Office, codes [redacted] are TIDE-only codes that are not included in the Terrorist Screening Database and cannot currently be used for vetting purposes.[5] In addition, interagency watchlisting guidance does not allow codes [redacted] to be provided to TSA for aviation worker vetting. TSA's VAD recognized that not receiving these codes represented a weakness in its program. VAD officials informed us that as part of its analysis efforts, VAD had independently identified derogatory information on some individuals, and subsequently determined that these individuals belonged to the missing categories. VAD officials informed us that without receiving these categories, TSA could not guarantee that it could consistently identify all questionable individuals. TSA officials believed that receiving these categories would at least give them an opportunity to monitor these individuals.

In 2014, the TSA Administrator signed an internal TSA policy memo to partially address this potential weakness. In addition to category codes [redacted] identified above, the TSA Administrator authorized his staff to request category codes [redacted] for vetting. TSA's policy memo states that individuals in such categories could pose potential threats to aviation security if TSA is not given a chance to examine the information and assess any potential associated risk.

[5] Classified derogatory information for subjects with an international nexus to terrorism is maintained in TIDE. Terrorist records that meet minimum substantive derogatory and identifying criteria requirements are exported to the Terrorist Screening Database, which serves as the U.S. Government's consolidated terrorist watchlist.

TSA Relies on Airports for Criminal History and Work Authorization Checks

Compared to the generally effective controls TSA had in place to link individuals with terrorism information, TSA lacked effective controls to ensure that aviation workers did not have disqualifying criminal histories and that they possessed lawful status and the authorization to work in the United States. Under current law and FBI policy, TSA is not authorized to perform recurrent criminal checks of aviation workers because aviation worker vetting is considered to be for non-criminal justice purposes. Therefore, TSA did not recurrently vet workers for criminal histories similar to the recurrent vetting it performed for terrorism information. Instead, it relied on airport operators to perform criminal history and work authorization checks with limited quality reviews. Ultimately, TSA had to deny credentials for 4,800 individuals whose work authorizations had been previously approved by airports because it was unable to verify their lawful status in the United States.

TSA did not have an adequate monitoring process in place to ensure that airport operators properly adjudicated credential applicants' criminal histories. Chapter 49 of the CFR, part 1542 and TSA Security Directive 1542-04-08G require airports to complete a fingerprint-based CHRC before approving an individual for unescorted access. 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.[6] However, TSA officials informed us that airport officials rarely or almost never documented the results of their CHRC reviews electronically. TSA inspectors may view the hardcopy results of a CHRC during TSA's annual security inspection at commercial airports. However, this is a limited review of as few as one percent of aviation workers. Without sufficient documentation, TSA cannot systematically determine whether individuals with access to secured areas of the airports are free of disqualifying criminal events.

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. Instead, 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. Current FBI law and policy prohibit TSA from conducting recurrent criminal checks of aviation workers because aviation worker vetting is considered to be for non-criminal justice purposes. However, TSA has planned a pilot of the FBI's "Rap Back" program in order to address the weakness of not having a recurrent criminal history records check. Under

[6] According to TSA officials, TSA inherited criminal history procedures that were developed prior to the formation of TSA. TSA has drafted a proposed rule intended to strengthen criminal history vetting. The proposed rule remains in the clearance process as of May 2015.

the program, TSA and/or the airports will receive automated updates from the FBI for new criminal history matches associated with individuals who have undergone criminal history records checks so that they might provide these results to airports for action. TSA is planning this pilot program for multiple airports in late 2015. Given recent incidents where aviation workers were charged with crimes such as smuggling illegal drugs or guns, recurrent vetting of criminal histories may help TSA identify criminals before they can pose a risk to transportation security.

As previously discussed, TSA's Security Directive required that airport operators first validate an individual's authorization to work in the United States before forwarding the individual's records to TSA for additional clearance. Based on TSA data, however, airports may not be consistently verifying that credential applicants possess the immigration status necessary to work in the United States. Typically, a person "authorized to work" has lawful status in the United States. If airport operators accurately performed the verifications prior to sending the applicants' records to TSA, there should be minimal discrepancies between an "authorized to work" check and a lawful status check.

However, according to program officials, TSA has had to send nearly 29,000 inquiries to credential applicants since program inception in 2004. These inquiries were necessary because TSA had questions about the applicants' lawful status. 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 already received clearance from the airports as being authorized to work. The magnitude of individuals "authorized to work" for whom TSA cannot confirm lawful status may indicate a control weakness in the airports' work verification process that should be addressed.[7]

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 may look 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.

[7] Since airports are required to collect and review documents validating an individual's right to work in the United States, those documents should contain evidence of lawful status as well.

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. Security Directive 1542-04-08G contains no requirement that airport operators limit the expiration date of an individual's credential to the last date they are eligible to work in the United States. Under the Security Directive, TSA required airports to verify work authorizations upon badge renewal every 2 years, or whenever another credential was requested. If an individual's authorization to work expired within a year or a month of the individual obtaining the credential, the individual would continue to be cleared for the credential because the airports did not put an expiration date on the credential consistent with the term of the work authorization. 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 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. Incomplete or inaccurate aviation worker data can hinder TSA's ability to identify individuals who may pose a risk to transportation security.

Vetting Databases Contain Incomplete or Inaccurate Biographic Information

Although TSA had implemented robust procedures, its vetting of terrorism information may be impacted by incomplete and inaccurate data. TSA Security Directive 1542-04-08G requires that TSA not initiate a security threat assessment of an applicant or current badge holder until the airport operators submit all biographic information for an individual, including the following:

- full legal first, middle and last name,
- gender,
- date of birth, and
- alien registration number or I-94 Arrival/Departure form number for non-U.S. citizens.

Despite these requirements, we identified records in TSA vetting databases that contained potentially inaccurate or missing data. Specifically, we identified over 1,500 records in TSA's screening gateway where an individual's first name contained two or fewer characters; over 300 contained a single character. We identified an additional 75,000 records where individuals with active aviation worker credentials were listed in the CSG as being citizens of non-U.S. countries, but did not have passport numbers listed. 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.

Through analysis of TSA data, we determined that nearly 87,000 active aviation workers did not have SSNs listed. Pursuant to the *Privacy Act*, TSA is not authorized to require the collection of SSNs, although TSA's data matching model identified the SSN as a strong matching element. TSA encouraged applicants to submit their SSNs during the application process; however, to the extent individuals applying for aviation worker credentials do not list their SSNs, TSA may be unable to identify additional strong matches for analysts to manually review.

For full details of potentially incomplete or inaccurate biographic information, refer to table 2.

Table 2: Potentially Incomplete or Inaccurate Biographic Information Provided to TSA

Data Issue	**Potentially Incomplete/Inaccurate Records**
First Names with 2 Characters or Less	1,500
No Alien Registration Number for Immigrants	14,000
No Passport Number for Immigrants[8]	75,000
No SSNs	87,000

Source: DHS OIG analysis of TSA data.

In addition to the data completeness issues that we identified, TSA had independently determined that airports may not be providing all aliases used by applicants undergoing security threat assessments. Complete and accurate aliases are important to the accuracy and effectiveness of TSA's vetting processes. As such, TSA had issued correspondence to airports stating that legal name changes, birth name changes, maiden names, and spelling variations must be listed on the credential applications, and that TSA would reject applications where it determined a second name existed that was not listed on the application. However, in some instances, TSA may not have been aware that aliases existed for specific individuals. To the extent that airports do not ensure that aliases are captured and provided to TSA, TSA terrorism vetting may be limited for those individuals.

[8] While TSA considered passports to be excellent proof for identity verification and work authorization, it allows individuals to present other documents in place of passports.

TSA has taken steps to address some of these weaknesses. Specifically, TSA made system enhancements between 2012 and 2014 designed to improve the quality of data that it received from airports. These enhancements included policies such as rejecting dates of birth that indicate an individual is 14 years of age or under, or older than 105 years, or encouraging airports to submit electronic copies of required immigration paperwork with applications, in order to expedite the threat assessment process. These enhancements will become effective for new or reissued badges, which should happen within 2 years as required by TSA's Security Directive.

Recommendations

We recommend that the TSA Acting Administrator:

Recommendation 1. Follow up on TSA's request to determine if its credential vetting program warrants the receipt of additional categories of terrorism related records.

Recommendation 2. Issue guidance requiring that TSA's annual security inspection process include verification of original documentation supporting airport adjudication of an applicant's criminal history and work authorization.

Recommendation 3. Pilot FBI's Rap Back program and take steps to institute recurrent vetting of criminal histories at all commercial airports.

Recommendation 4. Require airports to put an end date to credentials of individuals allowed to work in the United States temporarily.

Recommendation 5. Analyze TSA's denials of credentials due to lawful status issues to identify airports with specific weaknesses, and address these weaknesses with airport badging officials as necessary.

Recommendation 6. Implement all necessary data quality checks necessary to ensure that all credential application data elements required by TSA Security Directive 1542-04-08G are complete and accurate.

TSA Response

We obtained written comments on a draft report from the Acting Deputy Administrator for TSA. We have included TSA's comments, in their entirety, in appendix C. TSA concurred with all of the recommendations.

OIG Analysis of TSA Comments

Management Comments to Recommendation 1

TSA concurs with recommendation 1. TSA officials said TSA is coordinating with DHS to formulate its request to receive additional Terrorist Identities Datamart Environment (TIDE) records to carry out its statutory duties to assess threats to transportation. TSA anticipates completion of this action by the close of calendar year 2015.

OIG Analysis

The described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until TSA provides its formal written request to the Interagency Policy Committee for additional terrorism-related records, or evidence that such a request cannot be implemented.

Management Comments to Recommendation 2

TSA concurs with recommendation 2. TSA officials said TSA will take action to update the *Compliance Program Manual* to include a requirement for Transportation Security Inspectors to witness airport badging office review of applicant criminal history record checks (CHRC) and lawful status during a comprehensive inspection. The update is expected to be completed by September 30, 2015.

OIG Analysis

The described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until TSA provides an updated *Compliance Program Manual* containing additional requirements for the annual review of airport badging office checks of CHRCs and lawful status.

Management Comments to Recommendation 3

TSA concurs with recommendation 3. TSA officials said TSA plans to initiate an FBI Rap Back pilot in late 2015 to help ensure full implementation across all eligible TSA-regulated populations in the future.

OIG Analysis

The described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until TSA provides evidence that it has initiated a Rap Back pilot at commercial airports to provide recurrent vetting of aviation workers.

Management Comments to Recommendation 4

TSA concurs with recommendation 4. TSA officials said TSA will publish guidance, no later than September 30, 2015, to all federalized airports to ensure that airport badge offices deactivate badges promptly when an individual's temporary authorization to work in the United States is terminated.

OIG Analysis

The described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until TSA provides evidence it has issued guidance to federalized airports to ensure airport badging offices deactivate badges with temporary work authorizations that have terminated.

Management Comments to Recommendation 5

TSA concurs with recommendation 5. TSA officials said TSA will work with airport operators to further analyze denials related to lawful status and will use a risk-based approach to identify and address specific weaknesses, as necessary, by September 30, 2015. To conduct the analysis, TSA will review applicable records in TSA systems to identify denials based on lawful status, validate reasons for the denials, and issue guidance to airports to address any noted weaknesses.

OIG Analysis

The described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until TSA provides evidence of its review and any guidance issued to airports to address noted weaknesses.

Management Comments to Recommendation 6

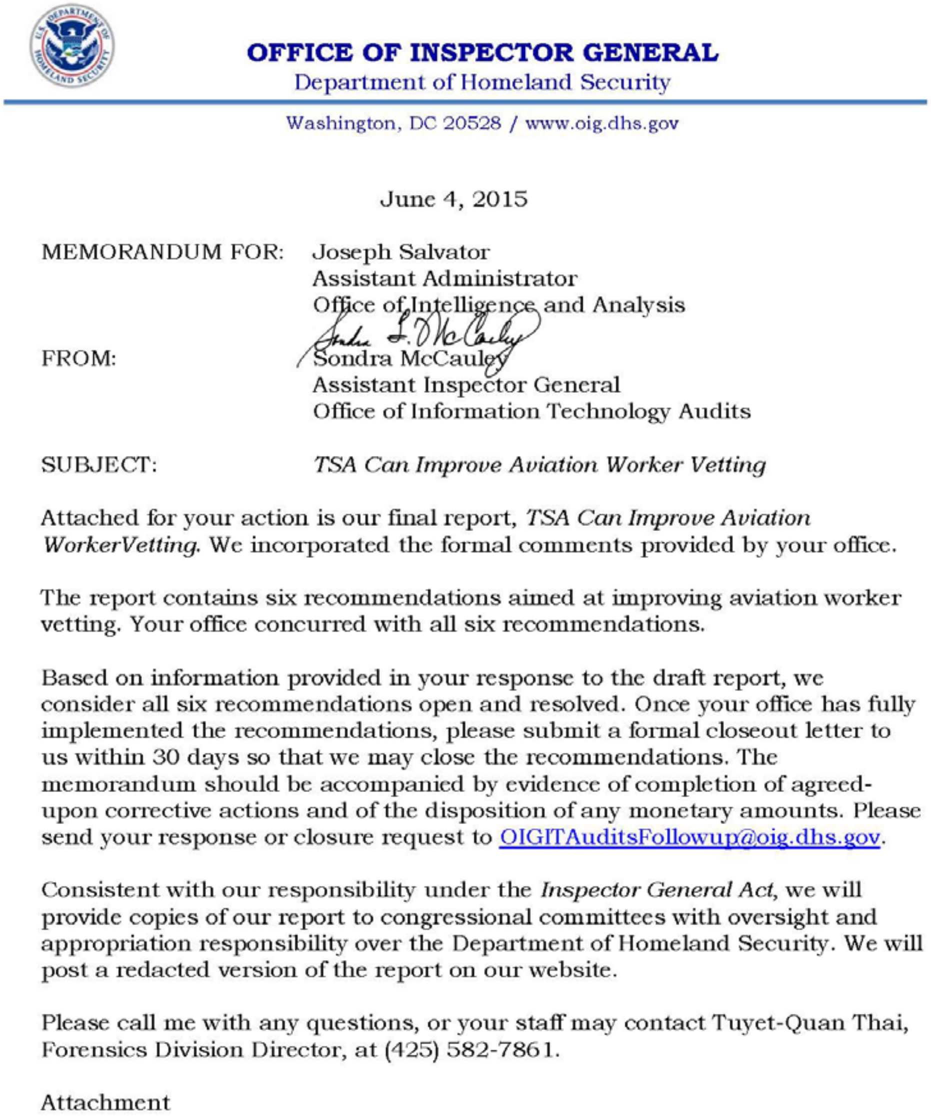
TSA concurs with recommendation 6. TSA officials said TSA will continue to work with airport operators to identify and correct data anomalies, and implement lessons learned to improve the quality of data received from airport operators for vetting purposes. TSA will review and analyze data submissions from airport operators and issue additional guidance to airport operators to address noted weaknesses by September 30, 2015.

OIG Analysis

The described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until TSA provides evidence of its review of airport operator data submissions and any guidance issued to airport operators to address noted weaknesses.

Appendix A

Transmittal to Action Official



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security
Washington, DC 20528 / www.oig.dhs.gov

June 4, 2015

MEMORANDUM FOR: Joseph Salvator
Assistant Administrator
Office of Intelligence and Analysis

FROM: Sondra L. McCauley
Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *TSA Can Improve Aviation Worker Vetting*

Attached for your action is our final report, *TSA Can Improve Aviation WorkerVetting*. We incorporated the formal comments provided by your office.

The report contains six recommendations aimed at improving aviation worker vetting. Your office concurred with all six recommendations.

Based on information provided in your response to the draft report, we consider all six recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGITAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted version of the report on our website.

Please call me with any questions, or your staff may contact Tuyet-Quan Thai, Forensics Division Director, at (425) 582-7861.

Attachment

Appendix B

Scope and Methodology

The Department of Homeland Security Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The objectives of our review were to identify potential enhancements to the TSA vetting process for individuals with access to secure areas of commercial airports and to determine the accuracy and reliability of data TSA uses to vet those individuals.

We reviewed applicable laws, regulations, and security directives concerning TSA's responsibilities in the vetting of individuals with access to secure areas of commercial airports. In addition, we reviewed prior OIG audit reports and U.S. Government Accountability Office reports on commercial airport security.

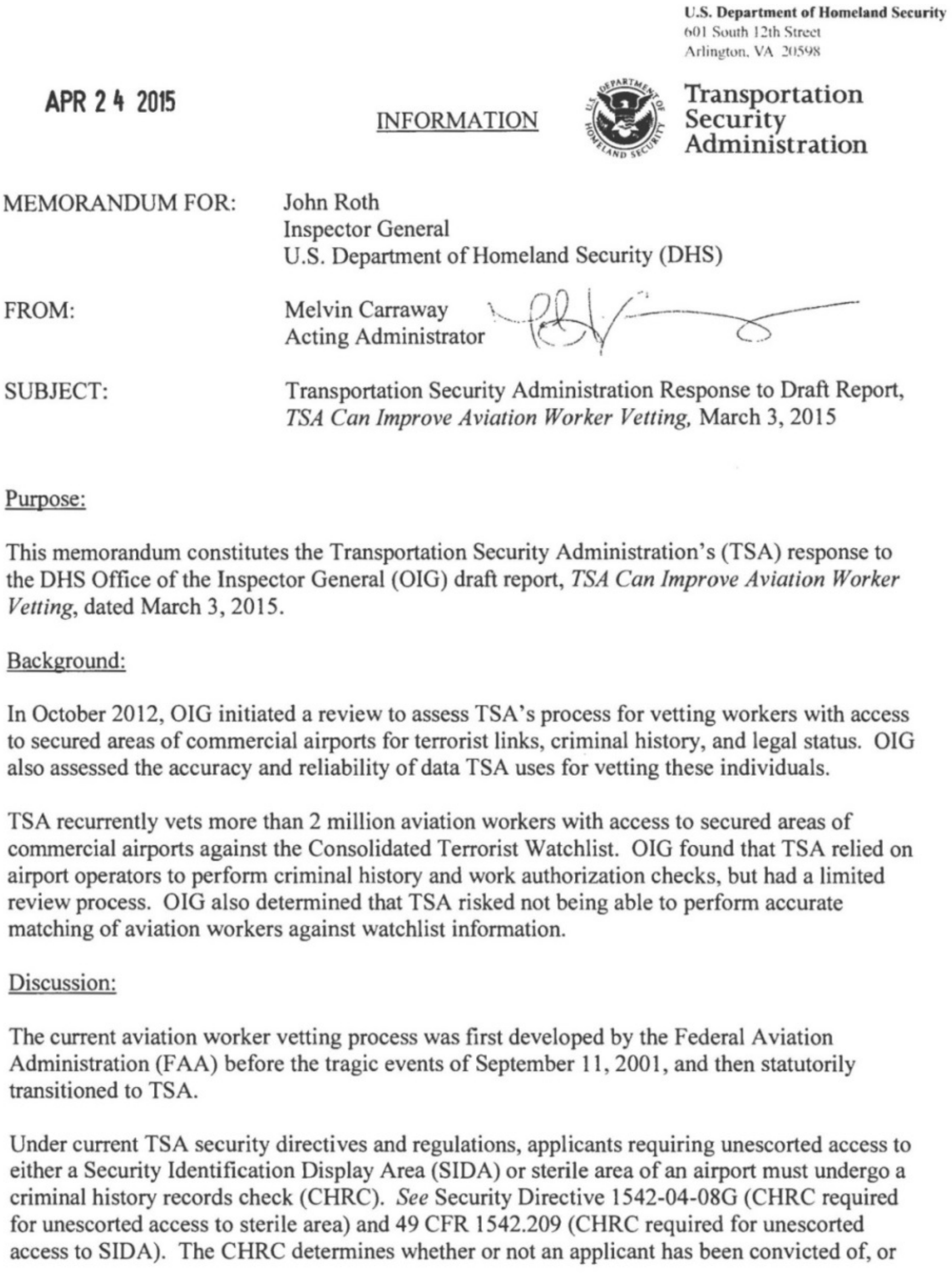
We conducted site visits in Colorado Springs, Colorado; Annapolis Junction, Maryland; and Herndon and Arlington, Virginia. During these site visits we interviewed TSA officials and walked through the control processes and procedures for vetting individuals applying for credentials granting unescorted access to secure areas of commercial airports. The processes and procedures we examined included automated and manual procedures for vetting individuals against terrorism information; the adjudications process for immigration and criminal history checks; the coordination, disposition, and monitoring of terrorism cases; and the identification of new terrorism subjects using nonobvious link analysis. We did not interview DHS Office of Policy's Screening Coordination Office.

We received full databases of individuals holding or applying for secure access credentials from the CSG and the VAD. We analyzed individuals' biographic data for accuracy and other data errors, and matched CSG data against VAD data to determine whether there was evidence that all individuals holding or applying for credentials were being vetted against terrorism information. We also collaborated with the National Counterterrorism Center 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.

We conducted this performance audit between May 2014 and February 2015 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.

Appendix C

TSA Comments to the Draft Report



U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598

Transportation Security Administration

APR 2 4 2015

INFORMATION

MEMORANDUM FOR: John Roth
Inspector General
U.S. Department of Homeland Security (DHS)

FROM: Melvin Carraway
Acting Administrator

SUBJECT: Transportation Security Administration Response to Draft Report, *TSA Can Improve Aviation Worker Vetting,* March 3, 2015

Purpose:

This memorandum constitutes the Transportation Security Administration's (TSA) response to the DHS Office of the Inspector General (OIG) draft report, *TSA Can Improve Aviation Worker Vetting*, dated March 3, 2015.

Background:

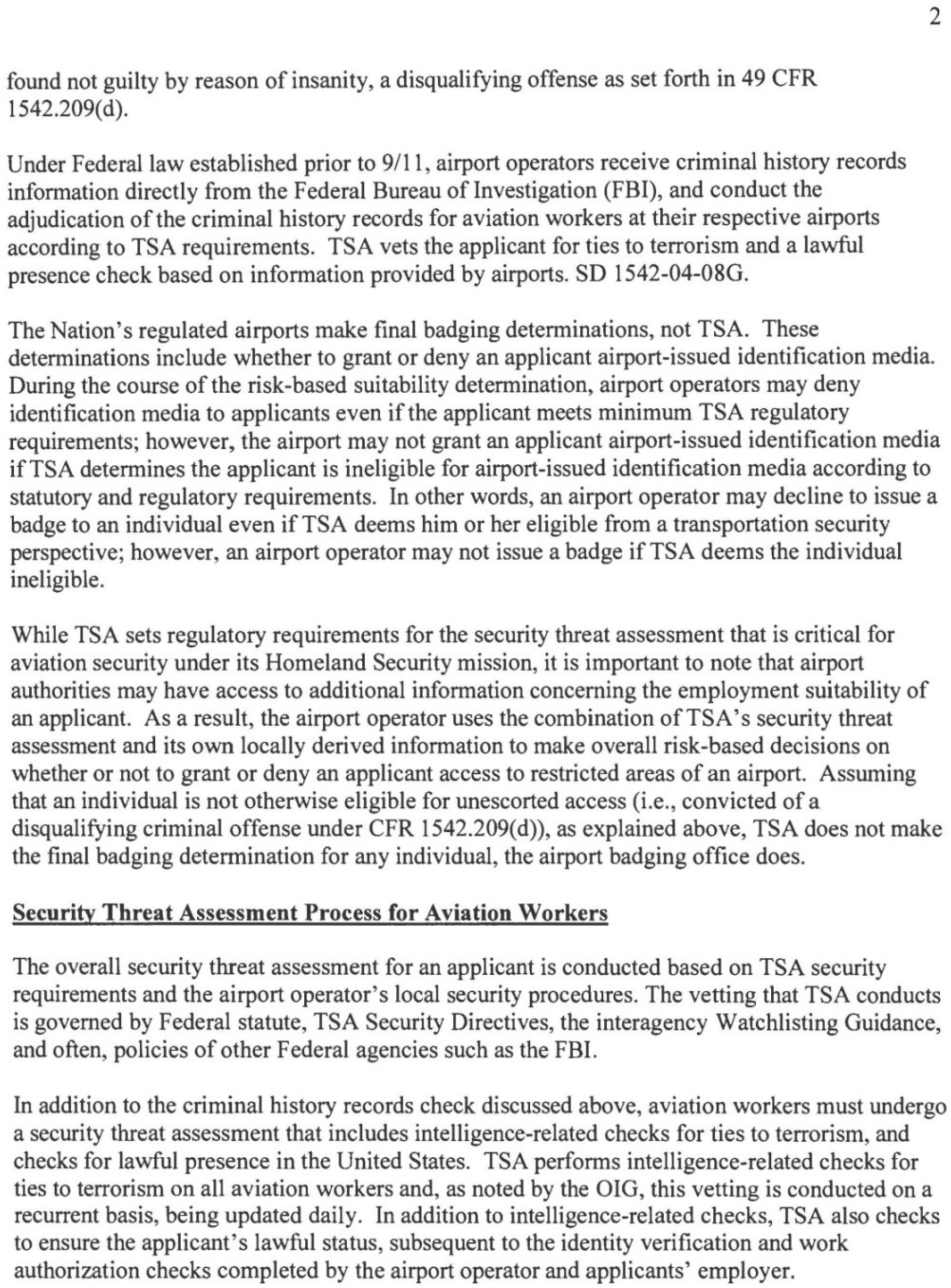
In October 2012, OIG initiated a review to assess TSA's process for vetting workers with access to secured areas of commercial airports for terrorist links, criminal history, and legal status. OIG also assessed the accuracy and reliability of data TSA uses for vetting these individuals.

TSA recurrently vets more than 2 million aviation workers with access to secured areas of commercial airports against the Consolidated Terrorist Watchlist. OIG found that TSA relied on airport operators to perform criminal history and work authorization checks, but had a limited review process. OIG also determined that TSA risked not being able to perform accurate matching of aviation workers against watchlist information.

Discussion:

The current aviation worker vetting process was first developed by the Federal Aviation Administration (FAA) before the tragic events of September 11, 2001, and then statutorily transitioned to TSA.

Under current TSA security directives and regulations, applicants requiring unescorted access to either a Security Identification Display Area (SIDA) or sterile area of an airport must undergo a criminal history records check (CHRC). *See* Security Directive 1542-04-08G (CHRC required for unescorted access to sterile area) and 49 CFR 1542.209 (CHRC required for unescorted access to SIDA). The CHRC determines whether or not an applicant has been convicted of, or



found not guilty by reason of insanity, a disqualifying offense as set forth in 49 CFR 1542.209(d).

Under Federal law established prior to 9/11, airport operators receive criminal history records information directly from the Federal Bureau of Investigation (FBI), and conduct the adjudication of the criminal history records for aviation workers at their respective airports according to TSA requirements. TSA vets the applicant for ties to terrorism and a lawful presence check based on information provided by airports. SD 1542-04-08G.

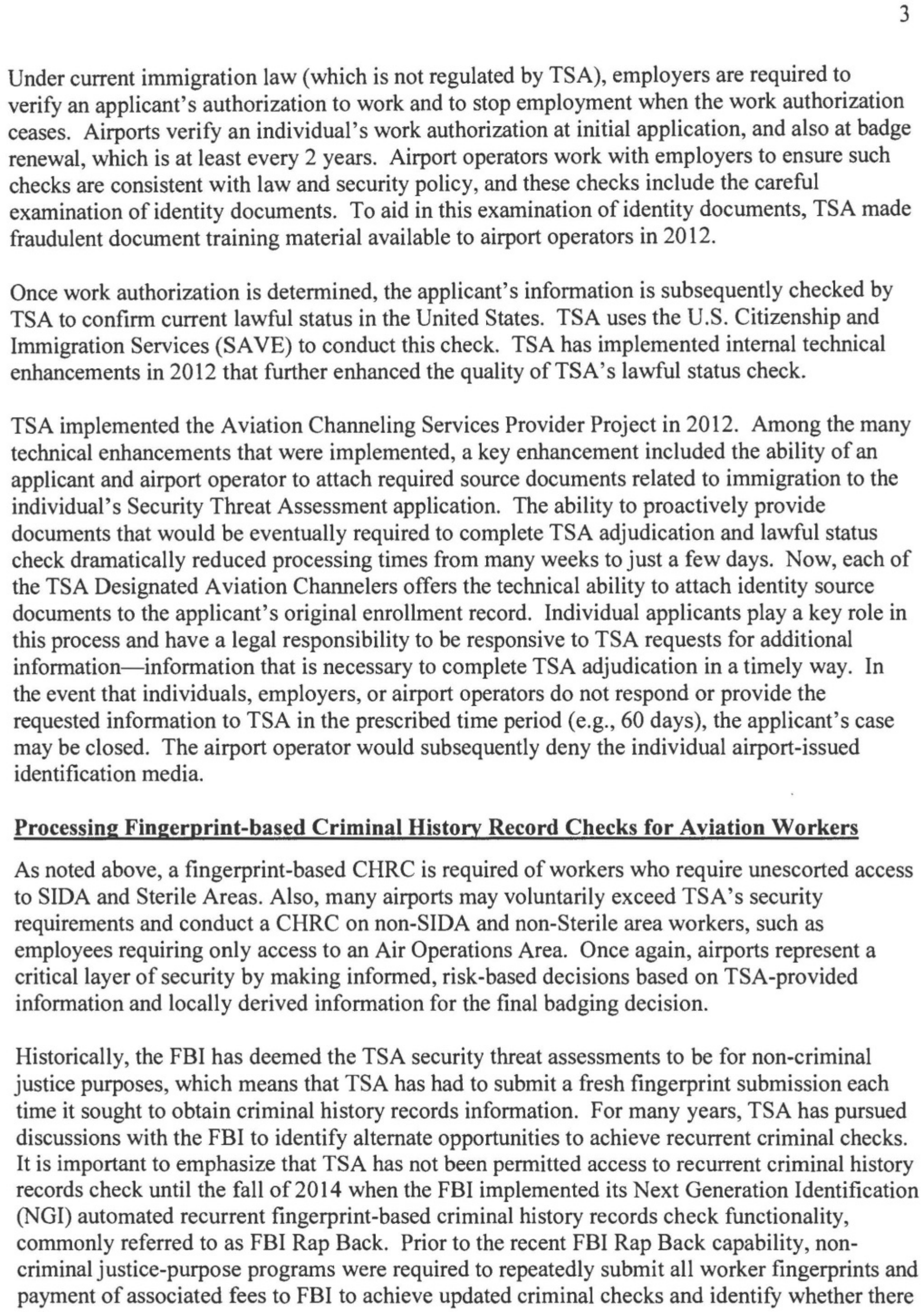
The Nation's regulated airports make final badging determinations, not TSA. These determinations include whether to grant or deny an applicant airport-issued identification media. During the course of the risk-based suitability determination, airport operators may deny identification media to applicants even if the applicant meets minimum TSA regulatory requirements; however, the airport may not grant an applicant airport-issued identification media if TSA determines the applicant is ineligible for airport-issued identification media according to statutory and regulatory requirements. In other words, an airport operator may decline to issue a badge to an individual even if TSA deems him or her eligible from a transportation security perspective; however, an airport operator may not issue a badge if TSA deems the individual ineligible.

While TSA sets regulatory requirements for the security threat assessment that is critical for aviation security under its Homeland Security mission, it is important to note that airport authorities may have access to additional information concerning the employment suitability of an applicant. As a result, the airport operator uses the combination of TSA's security threat assessment and its own locally derived information to make overall risk-based decisions on whether or not to grant or deny an applicant access to restricted areas of an airport. Assuming that an individual is not otherwise eligible for unescorted access (i.e., convicted of a disqualifying criminal offense under CFR 1542.209(d)), as explained above, TSA does not make the final badging determination for any individual, the airport badging office does.

<u>Security Threat Assessment Process for Aviation Workers</u>

The overall security threat assessment for an applicant is conducted based on TSA security requirements and the airport operator's local security procedures. The vetting that TSA conducts is governed by Federal statute, TSA Security Directives, the interagency Watchlisting Guidance, and often, policies of other Federal agencies such as the FBI.

In addition to the criminal history records check discussed above, aviation workers must undergo a security threat assessment that includes intelligence-related checks for ties to terrorism, and checks for lawful presence in the United States. TSA performs intelligence-related checks for ties to terrorism on all aviation workers and, as noted by the OIG, this vetting is conducted on a recurrent basis, being updated daily. In addition to intelligence-related checks, TSA also checks to ensure the applicant's lawful status, subsequent to the identity verification and work authorization checks completed by the airport operator and applicants' employer.



Under current immigration law (which is not regulated by TSA), employers are required to verify an applicant's authorization to work and to stop employment when the work authorization ceases. Airports verify an individual's work authorization at initial application, and also at badge renewal, which is at least every 2 years. Airport operators work with employers to ensure such checks are consistent with law and security policy, and these checks include the careful examination of identity documents. To aid in this examination of identity documents, TSA made fraudulent document training material available to airport operators in 2012.

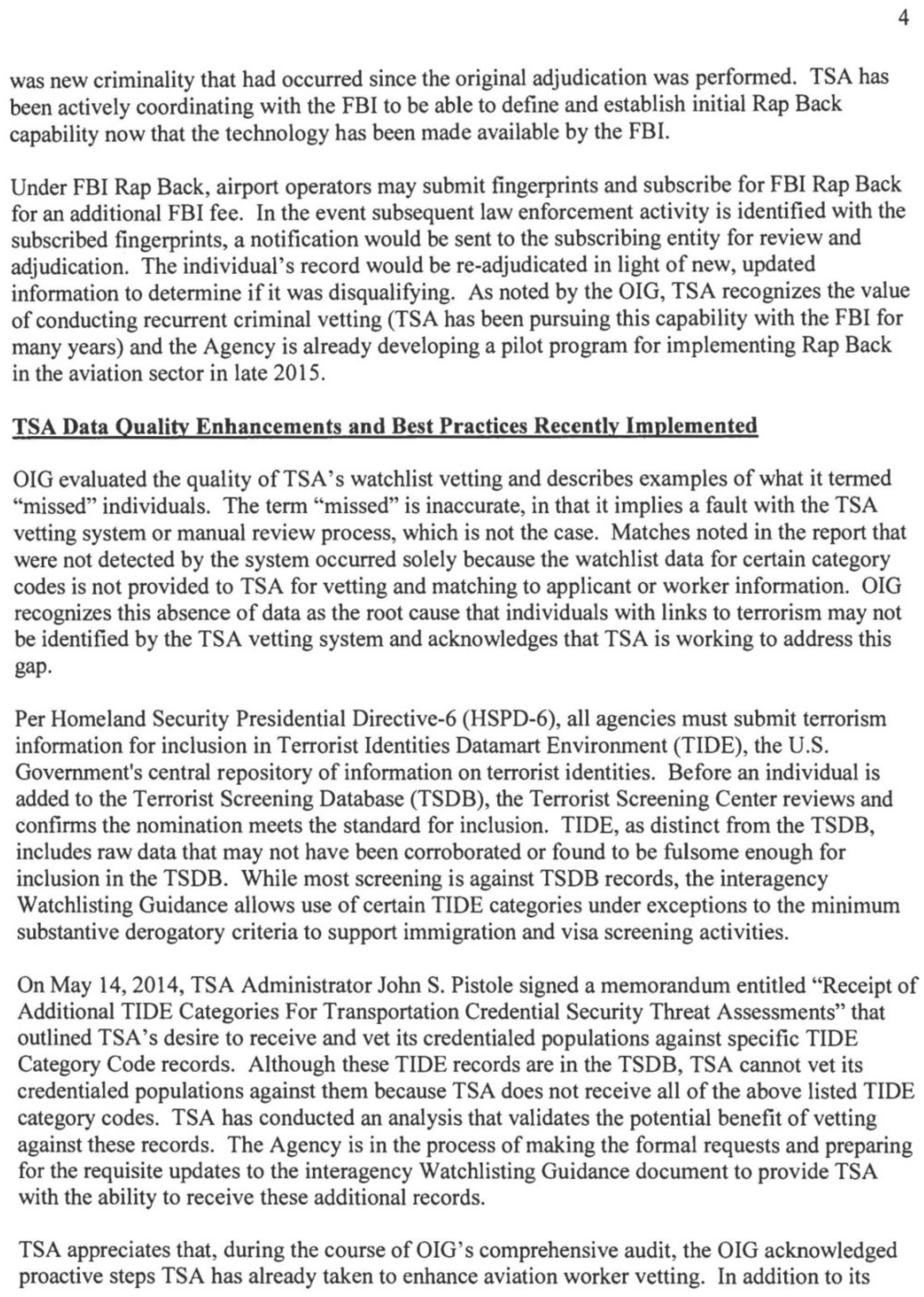
Once work authorization is determined, the applicant's information is subsequently checked by TSA to confirm current lawful status in the United States. TSA uses the U.S. Citizenship and Immigration Services (SAVE) to conduct this check. TSA has implemented internal technical enhancements in 2012 that further enhanced the quality of TSA's lawful status check.

TSA implemented the Aviation Channeling Services Provider Project in 2012. Among the many technical enhancements that were implemented, a key enhancement included the ability of an applicant and airport operator to attach required source documents related to immigration to the individual's Security Threat Assessment application. The ability to proactively provide documents that would be eventually required to complete TSA adjudication and lawful status check dramatically reduced processing times from many weeks to just a few days. Now, each of the TSA Designated Aviation Channelers offers the technical ability to attach identity source documents to the applicant's original enrollment record. Individual applicants play a key role in this process and have a legal responsibility to be responsive to TSA requests for additional information—information that is necessary to complete TSA adjudication in a timely way. In the event that individuals, employers, or airport operators do not respond or provide the requested information to TSA in the prescribed time period (e.g., 60 days), the applicant's case may be closed. The airport operator would subsequently deny the individual airport-issued identification media.

Processing Fingerprint-based Criminal History Record Checks for Aviation Workers

As noted above, a fingerprint-based CHRC is required of workers who require unescorted access to SIDA and Sterile Areas. Also, many airports may voluntarily exceed TSA's security requirements and conduct a CHRC on non-SIDA and non-Sterile area workers, such as employees requiring only access to an Air Operations Area. Once again, airports represent a critical layer of security by making informed, risk-based decisions based on TSA-provided information and locally derived information for the final badging decision.

Historically, the FBI has deemed the TSA security threat assessments to be for non-criminal justice purposes, which means that TSA has had to submit a fresh fingerprint submission each time it sought to obtain criminal history records information. For many years, TSA has pursued discussions with the FBI to identify alternate opportunities to achieve recurrent criminal checks. It is important to emphasize that TSA has not been permitted access to recurrent criminal history records check until the fall of 2014 when the FBI implemented its Next Generation Identification (NGI) automated recurrent fingerprint-based criminal history records check functionality, commonly referred to as FBI Rap Back. Prior to the recent FBI Rap Back capability, non-criminal justice-purpose programs were required to repeatedly submit all worker fingerprints and payment of associated fees to FBI to achieve updated criminal checks and identify whether there



was new criminality that had occurred since the original adjudication was performed. TSA has been actively coordinating with the FBI to be able to define and establish initial Rap Back capability now that the technology has been made available by the FBI.

Under FBI Rap Back, airport operators may submit fingerprints and subscribe for FBI Rap Back for an additional FBI fee. In the event subsequent law enforcement activity is identified with the subscribed fingerprints, a notification would be sent to the subscribing entity for review and adjudication. The individual's record would be re-adjudicated in light of new, updated information to determine if it was disqualifying. As noted by the OIG, TSA recognizes the value of conducting recurrent criminal vetting (TSA has been pursuing this capability with the FBI for many years) and the Agency is already developing a pilot program for implementing Rap Back in the aviation sector in late 2015.

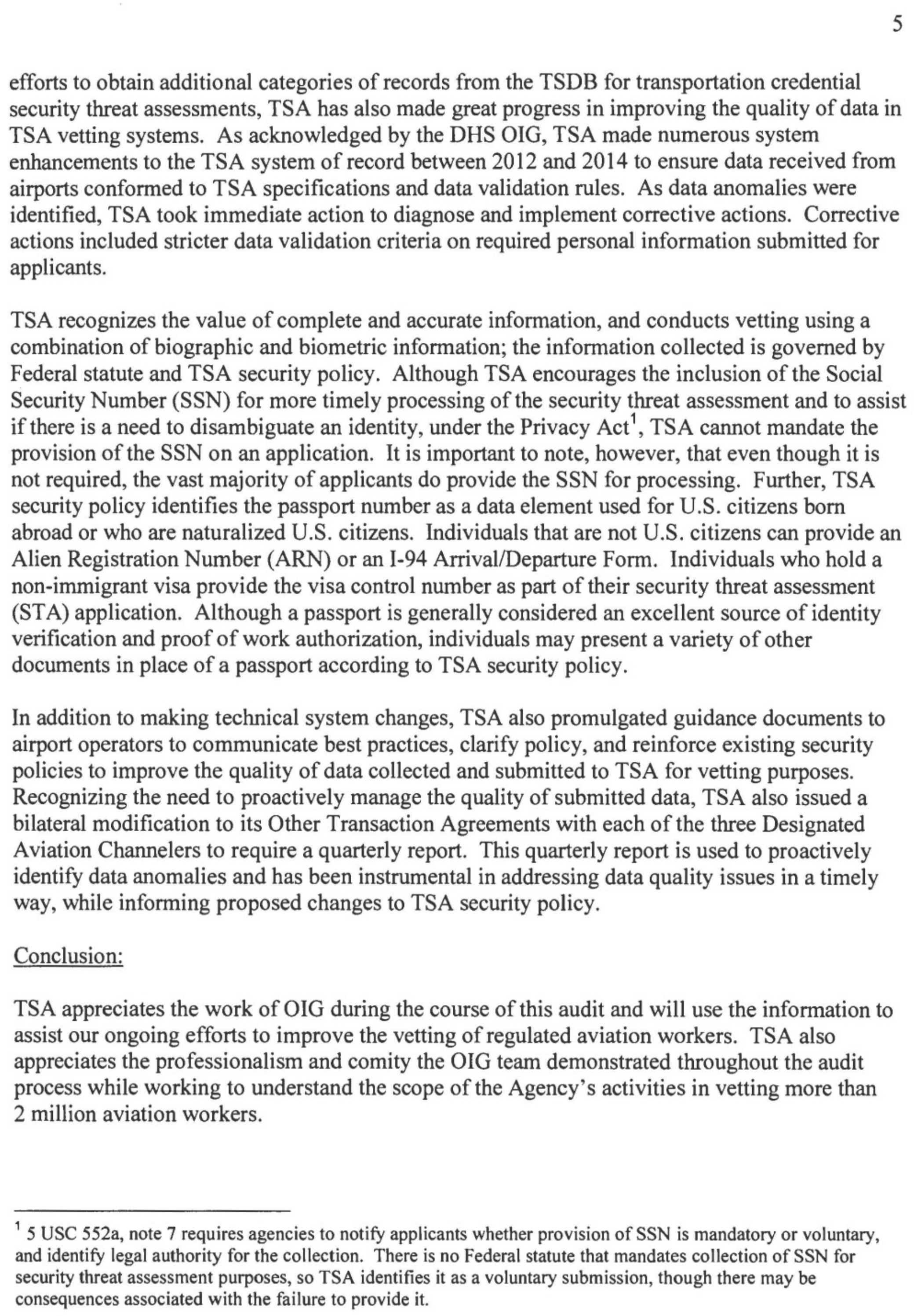
<u>TSA Data Quality Enhancements and Best Practices Recently Implemented</u>

OIG evaluated the quality of TSA's watchlist vetting and describes examples of what it termed "missed" individuals. The term "missed" is inaccurate, in that it implies a fault with the TSA vetting system or manual review process, which is not the case. Matches noted in the report that were not detected by the system occurred solely because the watchlist data for certain category codes is not provided to TSA for vetting and matching to applicant or worker information. OIG recognizes this absence of data as the root cause that individuals with links to terrorism may not be identified by the TSA vetting system and acknowledges that TSA is working to address this gap.

Per Homeland Security Presidential Directive-6 (HSPD-6), all agencies must submit terrorism information for inclusion in Terrorist Identities Datamart Environment (TIDE), the U.S. Government's central repository of information on terrorist identities. Before an individual is added to the Terrorist Screening Database (TSDB), the Terrorist Screening Center reviews and confirms the nomination meets the standard for inclusion. TIDE, as distinct from the TSDB, includes raw data that may not have been corroborated or found to be fulsome enough for inclusion in the TSDB. While most screening is against TSDB records, the interagency Watchlisting Guidance allows use of certain TIDE categories under exceptions to the minimum substantive derogatory criteria to support immigration and visa screening activities.

On May 14, 2014, TSA Administrator John S. Pistole signed a memorandum entitled "Receipt of Additional TIDE Categories For Transportation Credential Security Threat Assessments" that outlined TSA's desire to receive and vet its credentialed populations against specific TIDE Category Code records. Although these TIDE records are in the TSDB, TSA cannot vet its credentialed populations against them because TSA does not receive all of the above listed TIDE category codes. TSA has conducted an analysis that validates the potential benefit of vetting against these records. The Agency is in the process of making the formal requests and preparing for the requisite updates to the interagency Watchlisting Guidance document to provide TSA with the ability to receive these additional records.

TSA appreciates that, during the course of OIG's comprehensive audit, the OIG acknowledged proactive steps TSA has already taken to enhance aviation worker vetting. In addition to its



efforts to obtain additional categories of records from the TSDB for transportation credential security threat assessments, TSA has also made great progress in improving the quality of data in TSA vetting systems. As acknowledged by the DHS OIG, TSA made numerous system enhancements to the TSA system of record between 2012 and 2014 to ensure data received from airports conformed to TSA specifications and data validation rules. As data anomalies were identified, TSA took immediate action to diagnose and implement corrective actions. Corrective actions included stricter data validation criteria on required personal information submitted for applicants.

TSA recognizes the value of complete and accurate information, and conducts vetting using a combination of biographic and biometric information; the information collected is governed by Federal statute and TSA security policy. Although TSA encourages the inclusion of the Social Security Number (SSN) for more timely processing of the security threat assessment and to assist if there is a need to disambiguate an identity, under the Privacy Act[1], TSA cannot mandate the provision of the SSN on an application. It is important to note, however, that even though it is not required, the vast majority of applicants do provide the SSN for processing. Further, TSA security policy identifies the passport number as a data element used for U.S. citizens born abroad or who are naturalized U.S. citizens. Individuals that are not U.S. citizens can provide an Alien Registration Number (ARN) or an I-94 Arrival/Departure Form. Individuals who hold a non-immigrant visa provide the visa control number as part of their security threat assessment (STA) application. Although a passport is generally considered an excellent source of identity verification and proof of work authorization, individuals may present a variety of other documents in place of a passport according to TSA security policy.

In addition to making technical system changes, TSA also promulgated guidance documents to airport operators to communicate best practices, clarify policy, and reinforce existing security policies to improve the quality of data collected and submitted to TSA for vetting purposes. Recognizing the need to proactively manage the quality of submitted data, TSA also issued a bilateral modification to its Other Transaction Agreements with each of the three Designated Aviation Channelers to require a quarterly report. This quarterly report is used to proactively identify data anomalies and has been instrumental in addressing data quality issues in a timely way, while informing proposed changes to TSA security policy.

Conclusion:

TSA appreciates the work of OIG during the course of this audit and will use the information to assist our ongoing efforts to improve the vetting of regulated aviation workers. TSA also appreciates the professionalism and comity the OIG team demonstrated throughout the audit process while working to understand the scope of the Agency's activities in vetting more than 2 million aviation workers.

[1] 5 USC 552a, note 7 requires agencies to notify applicants whether provision of SSN is mandatory or voluntary, and identify legal authority for the collection. There is no Federal statute that mandates collection of SSN for security threat assessment purposes, so TSA identifies it as a voluntary submission, though there may be consequences associated with the failure to provide it.

U.S. Department of Homeland Security (DHS)
Transportation Security Administration (TSA)

Response to Draft Report, *TSA Can Improve Aviation Worker Vetting,* March 3, 2015

Recommendation No. 1: Aggressively follow up on TSA's request to the DHS Watchlist Service and obtain all watchlist information necessary for TSA to use for vetting aviation workers.

TSA concurs. TSA, in coordination with DHS, is in the process of formulating its request to receive additional Terrorist Identities Datamart Environment (TIDE) categories to carry out its statutory duties to assess threats to transportation. This request will require the interagency to agree to a change to the Watchlisting Guidance. TSA anticipates completion of this action by the close of calendar year 2015.

TSA did not request all TIDE categories identified in this audit. TSA requested only those TIDE categories that currently are exported to the Terrorist Screening Database (TSDB) to certain watchlist consumers. TSA did not request and does not plan to request TIDE categories that are currently exported to the TSDB as these categories have a more tenuous link to terrorism, and TSA has no plans to request them at this writing.

Recommendation No. 2: Issue guidance requiring that TSA's annual security inspection process include verification of original documentation supporting airport adjudication of an applicant's criminal history and legal status.

TSA concurs. TSA will take action to update the Compliance Program Manual to include a requirement for Transportation Security Inspectors to witness ID office employee review of applicant criminal history records checks (CHRC) and legal status during a comprehensive inspection. The update is expected to be complete by September 30, 2015.

Recommendation No. 3: Pilot FBI's Rap Back program and take steps to institute recursive vetting of criminal histories at all commercial airports.

TSA concurs. The criminal check will be recurrent, not "recursive." As indicated in the report, TSA plans to initiate an FBI Rap Back pilot in late 2015 in the aviation sector to inform Rap Back's full implementation across all eligible TSA-regulated populations in the future. Initiation of the pilot is dependent on the business, technical, and resource requirements for both TSA and pilot participants that TSA is in the process of defining.

Recommendation No. 4: Issue guidance to airport operators to ensure that airport employers submit badges for deactivation promptly when individuals' temporary authorizations to work end. (OIG revised this recommendation since draft report was published. This updated recommendation will be in final report.)

TSA concurs. TSA will publish guidance on the TSA ACO 200 Web Board no later than September 30, 2015, to all federalized airports to ensure that airport badge offices deactivate badges promptly when an individual's temporary authorization to work in the United States is terminated.

Recommendation No. 5: Analyze TSA's denials of credentials due to legal status issues to identify airports with specific weaknesses, and address these weaknesses with airport badging officials as necessary.

TSA concurs. TSA will work with airport operators to further analyze denials related to legal status and will use a risk-based approach to identify and address specific weaknesses with airport badging officials, as necessary, by September 30, 2015. To conduct the analysis, TSA will review applicable records in the TSA systems to identify denials related to legal status, validate the reasons for the denials, and issue guidance to airports to address any noted weaknesses.

Recommendation No. 6: Implement all necessary data quality checks necessary to ensure that all credential application data elements required by TSA Security Directive 1542-04-08G are complete and accurate.

TSA concurs. TSA will continue to work with airport operators to identify and correct data anomalies, and implement lessons learned to improve the quality of data received from airport operators for vetting purposes. TSA will review and analyze data submissions from airport operators and issue additional guidance to airport operators to address noted weaknesses by September 30, 2015.

Appendix D

Major Contributors to This Report

Tuyet-Quan Thai, Director, Forensics Division
Scott Wrightson, Audit Manager, Forensics Division
Charles Twitty, Referencer

Appendix E

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
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
TSA Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305