Department of Homeland Security
Office of Inspector General

TSA's Oversight of the Airport Badging Process Needs Improvement

(Redacted)

OIG-11-95

July 2011

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

JUL 07 2011

Preface

The Department of Homeland Security (DHS) 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.

This report addresses the strengths and weaknesses of the Transportation Security Administration's oversight to ensure that individuals who pose a threat are not granted access to secured airport areas. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Anne L. Richards
Assistant Inspector General for Audits

Table of Contents/Abbreviations

Appendixes

Abbreviations

AAAE	American Association of Airport Executives
CFR	Code of Federal Regulations
CHRC	criminal history records check
DHS	Department of Homeland Security
GAO	U.S. Government Accountability Office
OIG	Office of Inspector General
SIDA	Security Identification Display Area
STA	security threat assessment
TSA	Transportation Security Administration

Executive Summary

The Transportation Security Administration (TSA) is responsible for protecting the Nation's transportation systems. This includes ensuring that employees working in secured airport areas are properly vetted and badged. The agency relies on designated airport operator employees to perform the badging application process. Our objective was to determine whether the TSA provides effective oversight for the issuance of airport security badges.

Individuals who pose a threat may obtain airport badges and gain access to secured airport areas. We analyzed vetting data from 359 airport badging offices and identified [redacted] badge holder records with omissions or inaccuracies pertaining to security threat assessment status, birthdates, and birthplaces. For example, [redacted] of the badges were issued to individuals without a complete security threat assessment. These problems exist because TSA has designed and implemented only limited oversight of the application process. Specifically, the agency did not:

- Ensure that airport operators have quality assurance procedures for the badging application process;
- Ensure that airport operators provide training and tools to designated badge office employees; and
- Require its Transportation Security Inspectors to verify the airport data during their reviews.

Consequently, the safety of airport workers, passengers, and aircraft is at risk due to the potential of inappropriate individuals obtaining airport badges. TSA concurred with five recommendations and partially concurred with one that will improve the effectiveness of safeguards over the badging process.

Background

TSA is responsible for protecting the Nation's transportation systems. TSA has the statutory responsibility for requiring individuals with unescorted access to secure areas of the airport to be properly vetted. Secure airport areas include the following:

- Airport Sterile Area – The area of an airport that provides passengers access to boarding aircraft and to which TSA generally controls the access.
- Security Identification Display Area (SIDA) – The portion of an airport beyond the sterile area in which security measures are carried out.
- Air Operations Area – The aircraft movement areas, aircraft parking areas, loading ramps, and safety areas for use by aircraft.

In accordance with Title 49 Code of Federal Regulations (CFR) Part 1542, and TSA Security Directive 1542-04-08G, applicants are required to undergo a fingerprint-based criminal history records check (CHRC) and have an approved security threat assessment (STA) from TSA before receiving a badge and obtaining unescorted access to secure airport areas. TSA's Transportation Threat Assessment and Credentialing Vetting Operations is responsible for vetting individuals with unescorted access to secure areas. This is accomplished by comparing the applicant's information against critical data sets to discern whether the applicant is a threat to transportation or national security.

Criminal History Records Check *is a listing of certain information taken from fingerprint submissions retained by the Federal Bureau of Investigations in connection with arrests and, in some instances, federal employment, naturalization, or military service.*

Security Threat Assessment *is a check conducted by TSA of databases, including the terrorist watch lists, to confirm that an individual does not pose a security threat and possesses lawful status in the United States, and to verify an individual's identity.*

The Transportation Threat Assessment and Credentialing Vetting Operations annually vets approximately 550,000 individuals with

access to the secure airport areas. During vetting, changes to the data sets and watch lists are loaded into the system and compared with individuals' information stored in the vetting system. The system vets and provides immediate detection of a match against selected databases.

TSA's Threat Assessment and Credentialing adjudication service completes the STAs for applicants. The service works closely with intelligence, law enforcement, and other appropriate agencies to mitigate the potential insider threat. It relies heavily on the airports to input complete and accurate data.

TSA relies on Transportation Security Inspectors (Inspectors) to provide oversight of the airport badging process. Inspectors conduct various inspections, as well as assessments and investigations of the badging process, to determine compliance with the regulations. TSA requires Inspectors to perform an inspection of every airport and air carrier annually.

TSA also relies on designated airport operator employees as trusted agents to perform the essential functions of the badging process. Their duties consist of collecting, verifying, and inputting applicant data used for the STA process, and fingerprinting applicants for the CHRC. Airport operator employees are responsible for ensuring that the badge application is complete with the required biographical and fingerprint data for the STA and CHRC. Critical data processed from the application includes full legal name, date of birth, place of birth, passport number, and alien registration number. Appendix C lists the required application information.

Airport operator employees electronically transmit applicant data and fingerprints to the American Association of Airport Executives' (AAAE) Transportation Security Clearinghouse. AAAE provides a centralized aviation credentialing data exchange process to facilitate the vetting of aviation employees for TSA. AAAE is the data clearinghouse for approximately 359 airports

having formal access control programs. Approximately 890,000 individuals with 1.2 million active badges have access to secured airport areas.

Employees could have more than one badge if working for multiple employers at the airport.

Airport operator employees receive the applicant's clearance status from AAAE's Transportation Security Clearinghouse. If the STA and CHRC results are favorable, the airport operator employees will issue the badge with access to secured airport areas. Airports are responsible for ensuring that badges are issued only to qualified applicants and must account for and manage all active and deactivated badges. Appendix D presents a detailed diagram of the vetting process.

In 2007, U.S. Immigration and Customs Enforcement conducted a search at one major airport and arrested 23 workers with unauthorized airport access. This effort also identified more than 100 temporary employees possessing fraudulently obtained airport security badges. As a result, TSA's Office of Inspection reviewed the badging process and reported[1] vulnerabilities with training, technology, tools, and the CHRC process. Our 2008 report[2] also concluded that TSA needed to improve accountability over badges and TSA identification cards.

Results of Audit

Airport Badging Process Needs Improvement

Individuals who pose a threat may obtain airport badges and gain access to secured airport areas. We identified [redacted] badges issued to 95,961 individuals with one or more instances of omissions or inaccuracies of key applicant data used for vetting. For example [redacted] of the badges were issued to individuals without a complete STA. These problems existed because TSA has designed and implemented only limited oversight of the

[1] *Review of the Security Identification Display Area Badging Process*, (08-IRD-0004), April 2009.
[2] *Transportation Security Administration's Controls over SIDA Badges, Uniforms, and Identification Cards*, (OIG-08-92), September 2008.

application process. Specifically, TSA does not:

- Ensure that airport operators have quality assurance procedures for the badging process;
- Ensure that airport operators provide training and tools to designated badge office employees; and
- Require its Inspectors to verify the airport data during their reviews.

Consequently, the safety of airport workers, passengers, and aircraft is at risk due to the vulnerabilities in the airport operator badging process.

AAAE Data Are Inaccurate

Individuals are not always properly vetted and may inappropriately obtain airport badges and gain access to secured airport areas. AAAE provided us with a database of 1,187,630 active badges belonging to 889,354 individuals at 359 airports. Individuals could have more than one badge if working for more than one employer at the airport. We identified [redacted] badges issued to 95,961 individuals with one or more instances of omissions or inaccuracies[3] of key applicant data used for vetting, such as STA status, birthdates, and birthplaces. These badges were issued without the required information needed for vetting. Table 1 summarizes our analysis.

Table 1: AAAE Data Integrity

Type of Omission or Inaccuracy	Number of Badges Affected
STA Incomplete or Not Conducted	[redacted]
Date of Birth	[redacted]
Place of Birth	[redacted]
Inconsistent Citizenship	[redacted]
Total Data Problems Identified	[redacted]
[redacted].	

[3] For the purpose of this report, an omission is a blank data field and an inaccuracy is data that are inconsistent or falling outside established parameters of key biographical data used for vetting.

Many of the omissions or inaccuracies pertained to critical information used for vetting. For example, one applicant was listed as having three active badges at three different airports. The applications for this individual reflected three different places of birth: the United Kingdom, Ukraine, and the United States. We requested copies of the badging files for this individual from the three airports. He is a United States citizen and all three badging application files contained copies of his passport identifying the United Kingdom as his place of birth. TSA was unable to accurately vet the applicant against immigration information to determine legal status, yet the airports issued the badges. [redacted]

To further examine the integrity of the reported information, we requested data from 280 airport badging offices nationwide. TSA was unable to provide this information and directed us to request the reports from the airports. Only 193 airports were able to provide reports on their active badge holders in a timely manner. When comparing the airport reports with the AAAE database, we identified more than [redacted] individuals who possessed badges even though their records contained one or more omissions or inaccuracies.

Airport Badging Office Data Are Inaccurate

We visited 12 of the 193 airports and reviewed physical and electronic records belonging to 2,055 active badge holders. We compared and analyzed the information reported by AAAE with information at the airport badging offices. We identified [redacted] individuals with one or more instances of data omissions or types of inaccuracies who therefore should not have been issued a badge. For example—

- In [redacted] instances, there was no proof of an approved STA.
- Other items that were not correctly entered into the airport badging database and transmitted to AAAE included the

- applicants' full names, dates of birth, places of birth, passport numbers, alien registration numbers, or Social Security numbers.

At one airport, a record contained a questionable date of birth; however, the record belonged to an airport canine. According to airport officials, they had issued badges to working dogs in the past. Although we were informed that this is no longer standard practice, this canine was still listed as an active badge holder at the time of our visit.

Exhibit 1. Canines such as this one were previously issued badges.

Table 2 presents a summary of our analysis. Appendix E provides further details.

Table 2: Airport Visit Data Omissions or Inaccuracies

Type of Omission or Inaccuracy	Total Badges Affected
STA Inconsistencies	[redacted]
Date of Birth	[redacted]
Place of Birth	[redacted]
Name	[redacted]
Passport Number	[redacted]
Alien Registration Number	[redacted]
Social Security Number	[redacted]
Applications With Missing or Incomplete Data Fields	[redacted]
Total Omissions or Inaccuracies Identified	[redacted]
Individuals Involved Note: - Five contained two omissions or inaccuracies and one contained three.	[redacted]

Our review indicates that data omissions or inaccuracies could potentially lead to airports improperly issuing security badges. Additionally, we found that airports are not always collecting [redacted], even though many airport applications contain these data fields. We identified [redacted] records [redacted] and [redacted] records with incorrect [redacted]. These data elements are

additional unique identifiers that can assist in verifying an applicant's identity.

In response to our preliminary findings, the Airports Council International-North America[4] established a task force of its member airports to identify and evaluate best practices for airport identification badging. Some of the best practices identified included conducting audits of badging applications to identify common errors for incorporation into recurrent training classes, providing advanced training on fraudulent document identification and document handling procedures, establishing checks to prevent duplicate records, and establishing a quality control process to review applicant information before it is submitted for an STA.

Quality Assurance

TSA does not ensure that airport operators have quality assurance procedures to safeguard the completeness and accuracy of the data used for vetting. As the federal agency responsible for transportation security, TSA should use the U.S. Government Accountability Office's (GAO) Internal Control and Management Tool[5] for guidance. This document identifies the need for agencies to have relevant and reliable information in order to run and control operations.

Of the 12 airports we visited, the airport with the fewest omissions or inaccuracies established its own quality assurance procedures. This airport had several procedures that could be considered best practices, such as conducting onsite badge audits annually; using a supervisory review checklist to ensure that at least two agents handle each application; using equipment to check identification; and using local police to run criminal investigation checks on badge applicants.

As a quality assurance measure, separation of duties at some of the airport badging offices visited has resulted in more data accuracy.

[4] Airports Council International-North America is an industry trade organization representing local, regional, and state governing bodies that own and operate commercial airports in the United States and Canada.
[5] *GAO Internal Control Standards: Internal Control Management and Evaluation Tool*, GAO-01-1008G (August 2001).

Different individuals verifying information would likely enhance the detection of missing or inaccurate information, which affects the STA outcome. TSA's Security Directive 1542-04-08G requires airport operators to establish a process and identify the airport operator employees performing badging functions. The directive recommends, but does not mandate, different airport operator employees complete one of the following three tasks for each applicant:

- Collect and transmit the biographical and biometric information used in a CHRC and STA;
- Authorize the issuance of the badge; and
- Issue the badge.

Some sites we visited relied on best practices that could be implemented at other airports for ensuring authenticity of documentation and data accuracy. For example:

- One airport utilized daily system-generated reports to identify and resolve potential problems with active badge holders.
- One airport operator had a Memorandum of Understanding with U.S. Customs and Border Protection to have the agency verify all immigration documents before submitting the information to TSA for vetting.
- Another airport used a supervisory review checklist to ensure that at least two agents have reviewed the application for completeness and accuracy.

Training and Tools

Despite its reliance on the designated airport operator employees, TSA does not always ensure that airports are providing these individuals with proper training. Only one airport had a formalized training program focused on airport operator employees' duties and responsibilities. 49 CFR Part 1542 requires each airport operator to ensure that individuals performing security-related functions are briefed on specific requirements or guidance as they relate to the performance of their duties. Briefings must cover the provisions of 49 CFR Part 1542, security directives, information circulars, and airport security programs.

Airport operators and local TSA officials are not fully aware of the details of the complex vetting process and the ramifications of entering inaccurate biographical data. Officials at the 12 airports visited did not know what happens to the data once they enter the Transportation Security Clearinghouse. These officials did not realize how data entry errors or transposed numbers related to key identifying elements could create vulnerabilities, be exploited, and provide the wrong individuals access to secured airport areas. For example, an applicant with a birth date of January 21, 1965, which is incorrectly entered as January 21, 1956, could be vetted and approved for a badge.

TSA does not ensure that airport operator employees are using available tools while performing their assigned duties. At [redacted] airports visited, airport operator employees had tools available to assist in the identification of fraudulent documents but did not consistently use them. Tools include identification document scanners, ultraviolet lights, and loupes (magnifying lenses). These tools allow closer inspection of documents to prevent fraud.

[redacted] was not always using available tools such as an electronic scanner or lights and loupes to inspect documents submitted with badge applications. This location has a scanner that reads the magnetic strip on a driver's license or state-issued identification card and displays whether it is valid. When questioned, one employee admitted to using the scanner only occasionally but not using the lights and loupes at all. This employee was confident in their ability to identify fraudulent documentation without the use of these tools.

Figure 1 depicts an Alien Registration Card presented for identification. [redacted] does not stand out to the normal viewer [redacted]. However, using the appropriate tools and techniques, it is apparent [redacted]

We identified that training and use of tools such as lights and loupes to identify fraudulent documentation is effective. Trusted agents at one airport prevented four individuals from using fraudulent identification to obtain an airport badge. These individuals were prevented from obtaining badges because the trusted agents received fraudulent document training from the U.S. Customs and Border Protection and used lights and loupes to verify the authenticity of the documents submitted.

TSA Inspection Process

TSA's Inspectors review the airport badging process during inspections; however, the limited coverage does not ensure that vetting information is complete and accurate. TSA's Inspections Handbook and the Performance and Results Information System[6] provide Inspectors with basic questions and guidance based on regulatory requirements from the CFR and TSA Security Directives.

The handbook does not require the Inspectors to verify the information reported to TSA to identify discrepancies with badging

[6] TSA uses the Performance and Results Information System for factual and analytical information, monitoring compliance, measuring performance, assessing the efficiency and effectiveness of operations, and conducting inquiries into allegations of noncompliance with statutory or regulatory requirements.

information. It indicates that Inspectors should review employee files to ensure that all proper documentation has been submitted and returned to the airport operator before an employee is granted unescorted access to the secured area. Additionally, TSA does not require an established number or percentage of files to be reviewed as part of the inspection. Therefore, inspections of badging office records may be insufficient to determine the airports' level of compliance with vetting process requirements.

We reviewed the results of one annual inspection from 2010 related to the badging process and noted that the methodology did not provide an accurate conclusion. For example, the inspection reviewed compliance with issuing replacement badges when the badge holder provides a written declaration that the badge was lost, stolen, or destroyed. The Inspector concluded that the airport operator was compliant on the basis of an interview, without sufficient evidence of written declaration as a documentary review.

Inspectors do not always have direct access to the Transportation Security Clearinghouse database and are not required to compare or cross-reference records. To increase inspection effectiveness and efficiency, direct access to the clearinghouse data would enable Inspectors to verify records for approved STAs timely and take immediate corrective action if necessary. Because verification of applicant records against the clearinghouse information is not required during the inspection process, TSA did not arrange for Inspectors to have access to the data.

We presented all of our findings to the airport operators, local TSA officials, and Inspectors. Our analysis generated 101 updates, which airport operators sent to the Transportation Security Clearinghouse. We also provided a list of employees with suspect STAs beyond our random sample for follow-up, which prompted the Inspectors to take corrective action at some locations. For example, Inspectors at one airport revealed an additional 154 badges issued without accurate or complete vetting data. As a result, they immediately revoked access pending an approved STA.

Recurrent Criminal History Records Checks

TSA does not require airports to conduct recurring CHRCs to ensure that badge holders maintain their reputable status. According to 49 CFR Part 1542, an applicant must undergo a fingerprint-based CHRC before receiving a badge or obtaining unescorted access authority. If a badge holder is convicted of a disqualifying criminal offense after receiving a badge, he or she must report the offense and surrender the badge within 24 hours of a conviction or a finding of not guilty by reason of insanity. Appendix F presents a list of disqualifying crimes.

According to Security Directive 1542-04-08G, badges must be renewed at least every two years. For a badge renewal, employees must bring an application along with valid identification documentation to the airport badging office.

According to airport and TSA officials, the CHRCs should be conducted on a recurrent basis. These officials indicated that the self-reporting policy is ineffective because most employees would not report themselves for fear of losing their job.

Some airports have proactive measures to mitigate the risk involved with the CHRC process. For example, one airport had a private detective check 100 names per month for new outstanding warrants that may not have been self-reported.

Passing an initial CHRC does not preclude employees from engaging in subsequent criminal activity and presenting an insider threat at airports. For example, in 2007, a major news network reported that a customer service agent with no prior record was found guilty of several instances of accepting bribes totaling $21,500 from an undercover agent. The individual agreed to smuggle $396,000 along with illegally exporting weapons, military night vision goggles, and a cellular phone "jammer" to a foreign country. That same year, two workers at another airport were arrested after bringing guns and drugs on a flight. One worker was able to stow the guns and drugs near the departure gate ramp after using his airline uniform and badge to bypass TSA security.

Once a person engages in criminal behavior, he or she is more likely to continue similar or more egregious actions. The individual could also be easily influenced by bribery or coercion and pose an insider threat. Studies have shown that past behavior often corresponds to future criminal activity. A recidivism study[7] concluded that convicted criminals had a reconviction rate of 39% and overall reincarceration rate of 22%.

According to TSA officials, the agency recognizes the need for more frequent criminal checks. The Transportation Threat Assessment and Credentialing office, in cooperation with the agency's Office of Chief Council, is exploring implementation of a requirement to conduct CHRCs on a recurrent basis.

Conclusion

TSA's oversight of the airport badging process needs improvement. Only 193 of the 280 airports were able to provide reports showing active badge holders for their locations. Unless airport operators implement quality assurance procedures for the badging process, the data integrity and vetting results are questionable. TSA needs to ensure that airports are providing airport operator employees with the proper training and tools to perform their assigned duties and responsibilities. The agency's inspection activities must be enhanced in order to identify application omissions or inaccuracies for immediate corrective action.

Recommendations

We recommend that the Assistant Administrator, Office of Security Operations for the Transportation Security Administration:

Recommendation #1: Require that all airports having formal access control programs establish and implement quality assurance procedures to ensure:

- The accuracy and completeness of vetting information, and
- Airport personnel conduct their own verifications of approved applications.

[7] State of Connecticut Recidivism Study Annual Report, March 1, 2007.

Recommendation #2: Require that all airports having formal access control programs ensure that airport operator employees utilize all available tools to verify the identity of applicants. Also, encourage airports to collect passport and Social Security numbers from applicants, as these are unique identifiers that can assist and expedite the application process.

Recommendation #3: Develop and provide standardized training on identification verification and require airport operator employees to complete this training on a recurrent basis. The training can be developed in collaboration with other DHS agencies with expertise in correctly identifying immigration documentation.

Recommendation #4: Revise the Transportation Security Inspector Handbook to improve the oversight of the vetting process by requiring independent verifications of approved applications to enhance the quality of the data. This will ensure that data in the airport badging system and supporting databases are consistent with the information from the hard copy applications.

Recommendation #5: Provide Transportation Security Inspectors with real time reports generated from the existing database of all active badge holders for analysis. These reports should include an analysis identifying possible records with data inaccuracies based on factors such as age and duplicate personal identification numbers. The reports should provide the agency with immediate capabilities to effectively monitor and track the clearance process.

Recommendation #6: Require airports to conduct a criminal history records check for each badge holder on a recurrent basis to correspond with badge renewal. This will ensure that individuals who have committed disqualifying crimes no longer have access to secured airport areas.

Management Comments and OIG Analysis

TSA concurred with five recommendations and concurred in part with one. The agency acknowledged that our audit information

will be used to improve the efficiency and effectiveness of the airport badging process. TSA provided specific comments to the report and recommendations. A copy of TSA's written response is included in Appendix B. We summarized and addressed these comments below.

Response to Recommendation #1

TSA Concurred: TSA explained that Security Directive 1542-04-08G enhanced the security threat assessment process with the verification and use of biographic and biometric information. TSA also indicated the agency will review the quality assurance procedures for consistency across airports along with the vetting and verification process. The agency acknowledged that airport "self-assessments" could provide an additional security measure that would need to be supplemented by its own validation of approved applications.

OIG Analysis: As part of TSA's review of airport quality assurance procedures, the agency should focus on procedures to guarantee data integrity. Specifically, TSA must create or revise a security directive to ensure that there is a separation of duties between data entry and validation. This recommendation is unresolved until TSA provides a copy of the directive or other tool to be used for evaluating airport quality assurance procedures. Upon reviewing the documentation, we will close this recommendation after determining that it meets the intent of this recommendation.

Response to Recommendation #2

TSA Concurred: TSA indicated that oversight can be provided through periodic inspections to ensure that airport operator employees utilize all available tools to verify the identity of applicants and to encourage airports to collect passport and Social Security numbers from applicants.

TSA's Security Directive 1542-04-08G advises airport operators that providing Social Security numbers expedites the STA process.

OIG Analysis: TSA's response to this recommendation did not fully address the issue of airport operators collecting passport numbers which would also facilitate the STA process. This recommendation is unresolved until TSA provides documentation to support the agency's (1) plan to confirm that airport operators are properly utilizing all available tools to verify the identity of applicants and (2) updated security directive, which also includes the collection of passport numbers (when available), by airport operators when submitting information for the vetting process. We will close the recommendation once the agency has provided sufficient evidence of corrective actions that satisfy the recommendation.

Response to Recommendation #3

TSA Concurred: TSA plans to develop and provide standardized training on identification verification. The agency will explore ways to assist airport operators in improving identification verification for airport badge applicants. This includes a collaborative effort with U.S. Customs and Border Protection and U.S. Citizenship and Immigration Services to develop training for detection of fraudulent documents. Additionally, TSA indicated the agency is developing a proposed rule to improve and standardize STA processes and criteria. This proposed rule is supposed to include a provision for training personnel who conduct identity verification.

OIG Analysis: TSA's response included efforts to help identification training; however, the agency did not fully address the intent of the recommendation for recurrent training. This recommendation is unresolved until TSA provides a corrective action plan with dates of completion and names of the responsible officials. We will close the recommendation once TSA provides a copy of the enhanced training materials, the finalized STA rule, and the agency's plan for recurrent training in this area.

Response to Recommendation #4

TSA Concurred: TSA indicated that it will continue to review the Transportation Security Inspector Handbook to further develop the inspection methodology for STAs. The agency has identified potential enhancements such as the collection of required personal data, proper maintenance of personal data in the airport badging system database, consistency with dates in the database and on hard copy applications, and checking an employee's "cleared" status prior to granting them unescorted access to secured airport areas.

OIG Analysis: This recommendation is unresolved until TSA provides a corrective action plan with dates of completion and names of the responsible officials. This recommendation will remain open until TSA provides a copy of the revised Transportation Security Inspector Handbook with the improved methodology for the STAs.

Response to Recommendation #5

TSA Concurred: TSA partially concurred with this recommendation because the capability for providing Inspectors with real-time badging data does not currently exist. The agency's response explained that obtaining such real-time data would require a feasibility study and additional coordination.

OIG Analysis: During our audit, we obtained and demonstrated the benefit of having real-time reports generated at the local airport level. Using current information, an inspection could review the population of badge holders and identify questionable data, focusing on potential improperly cleared individuals. This recommendation is unresolved until TSA provides a corrective action plan with dates of completion and names of the responsible officials. We will close this recommendation when TSA provides evidence that Inspectors will access real time local badging information for use in monitoring and tracking the clearance process.

Response to Recommendation #6

TSA Concurred: TSA is developing a proposed rule to improve and standardize STA processes and criteria. According to TSA, this rule will propose a standard duration for all STAs. Upon STA expiration, the individual would need to reapply, and the STA checks, including the CHRC, would be repeated. This proposed rule is still in the coordination process.

OIG Analysis: This recommendation is unresolved until TSA provides a corrective action plan with dates of completion and names of the responsible officials. This recommendation will remain open until TSA provides a copy of the finalized rule and we have determined that it meets the intent of this recommendation.

The objective of our audit was to determine whether the TSA provides effective oversight for the issuance of airport security badges. To achieve our objective, we reviewed prior audit reports to identify any related findings and recommendations. We researched legislation such as the *Homeland Security Act of 2002*, 49 CFR parts 1542 and 1544, Security Directive 1542-04-08G, and other related security directives. We reviewed TSA annual inspections, special emphasis inspections, and airport standard operating procedures to identify documented weaknesses in the badging process.

We interviewed officials from various TSA offices, including Transportation Threat and Credentialing, Adjudication Center, Colorado Springs Operations Center, Office of Security Operations, Office of Inspection, and Transportation Sector Network Management. We interviewed officials from AAAE to understand their role in the vetting process and to request database information for all active badge holders. AAAE provided the following fields: last name, first name, middle name, date of birth, place of birth, citizenship, Social Security number, alien registration number, passport number, and passport-issuing country. These data fields are crucial to the vetting process and data for the same fields were requested from more than 280 airport badging offices nationwide.

We received data on 616,977 active badges belonging to 598,118 individuals from 193 of the 280 badging offices. We attempted to obtain specific badging information from all of the airports reporting to AAAE; however, we were unable to do so as TSA could not directly obtain this information. We then requested the information from the airports, not all of which could provide it. We compared the airport badging system reports with the AAAE data. We assessed the reliability of key data elements by confirming dates of birth and personal identification numbers such as passport numbers and alien registration numbers.

We selected 12 airports with high numbers of badged employees, and some locations with close proximity to the borders. We interviewed Federal Security Directors, Assistant Federal Security Directors, Transportation Security Inspectors, Airport Security

Coordinators, and designated airport operator employees, or trusted agents. For the 12 airports, we reviewed a total of 241,582 records. We also selected a statistically valid sample size of physical records to review using IDEA software. Using a 95% confidence level, 5% sampling error, and 50% population proportion, the required sample size was 384. We reviewed additional records and compared a minimum of 100 employee records at each site, as shown in Table 3. We cross-referenced hardcopy applications to the airport badging database. The airports used our analysis to update AAAE and also deactivated, revoked, or reissued some badges, depending on the results.

Table 3. Airports Visited and Analysis Results

Airport	Number of Statistical Records Reviewed	Number of Judgmental Records Reviewed	Total Hardcopy Records Reviewed
[redacted]	60	40	**100**
[redacted]	10	94	**104**
[redacted]	98	2	**100**
[redacted]	13	87	**100**
[redacted]	6	94	**100**
[redacted]	10	90	**100**
[redacted]	22	78	**100**
[redacted]	7	93	**100**
[redacted]	113	0	**113**
[redacted]	5	95	**100**
[redacted]	29	71	**100**
[redacted]	11	89	**100**
Totals	**384**	**833**	**1,217**

We conducted this performance audit between October 2010 and January 2011 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.

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

Transportation Security Administration

MAY 18 2011

INFORMATION

MEMORANDUM FOR: Anne L. Richards
Assistant Inspector General for Audits
U.S. Department of Homeland Security (DHS)

FROM: John S. Pistole
Administrator

SUBJECT: *TSA's Oversight of the Airport Badging Process Needs Improvement – Sensitive Security Information (SSI)*
OIG Project No. 10-154-AUD-TSA

Purpose

This memorandum constitutes the Transportation Security Administration's (TSA) response to the DHS Office of the Inspector General (OIG) draft report entitled *TSA's Oversight of the Airport Badging Process Needs Improvement – Sensitive Security Information (SSI)*, OIG Project No. 10-154-AUD-TSA, dated April 5, 2011.

Background

Between October 2010 and January 2011, OIG conducted a review to determine whether TSA provides effective oversight for the issuance of airport security badges and if individuals who pose a threat may obtain airport badges and gain access to secured airport areas. Overall, the OIG concluded that TSA's oversight of the airport badging process needs improvement.

Discussion

TSA appreciates OIG's work in completing this audit and will use the information in the audit to assist our ongoing efforts to improve the efficiency and effectiveness of the airport badging process. TSA is already implementing solutions that address several recommendations contained in the report. With regard to OIG's six recommendations, TSA responds as follows:

Recommendation #1: Require that all airports having formal access control programs establish and implement quality assurance procedures to ensure:

- The accuracy and completeness of vetting information, and
- Airport personnel conduct their own verifications of approved applications.

TSA Concurs. TSA's Security Directive (SD) 1542-04-08G enhanced the security threat assessments (STAs) process by requiring airport operators to verify and use trusted agents for collection and processing of biographic and biometric information. TSA will review the quality assurance procedures for consistency across airports along with the vetting and verification process. While "self-assessment" could provide an additional security measure, TSA would still need to validate compliance so an airport operator is not the sole point of validation for verification of approved applications.

Recommendation #2: Require that all airports having formal access control programs ensure that airport operator employees utilize all available tools to verify the identity of applicants. Also, encourage airports to collect passport and Social Security numbers from applicants, as these are unique identifiers that can assist and expedite the application process.

TSA Concurs. While TSA can provide oversight and periodic inspections regarding available tools and their proper use, accountability for the proper use and implementation of those tools during the application process remains with the airport and its trusted agents. TSA's Security Directive 1542-04-08G advises airport operators that providing social security numbers helps speed up the STA process.

Recommendation #3: Develop and provide standardized training on identification verification and require airport operator employees to complete this training on a recurrent basis. The training can be developed in collaboration with other Department of Homeland Security components with expertise in identifying immigration documentation.

TSA Concurs. TSA continues to explore ways to assist airport operators in improving identification verification for airport badge applicants. TSA provided training and tools (black light and loupe) in a 2009 presentation to airport operators regarding fraudulent document identification. TSA continues to encourage voluntary use of e-Verify.

TSA is working with U.S. Customs and Border Protection and U.S. Citizenship and Immigration Services to develop additional training in the detection of fraudulent documents. In addition, TSA is developing a proposed rule to improve and standardize the processes and criteria used for almost all of the STAs conducted under TSA's regulations, including STAs for airport workers. This rulemaking, often referred to as the "Universal Rule," will address all aspects of the STA process, including the processes for verifying the identity of the STA applicants. The rule, which is still in coordination, will also propose training for personnel who conduct identity verification. We believe this initiative will address this recommendation.

Recommendation #4: Revise the Transportation Security Inspector Handbook to improve the oversight of the vetting process by requiring independent verifications of

approved applications to enhance the quality of the data. This will ensure that data in the airport badging system and supporting databases are consistent with the information from the hard copy applications.

TSA Concurs. TSA currently inspects airport operators to ensure that persons with unescorted access authority have undergone and properly cleared an STA and that the STA files are complete and properly documented with timely submissions. While TSA does not have the capacity to independently verify every application, TSA will continue to review the Transportation Security Inspector Handbook to further develop the inspection methodology for STAs. Possible enhancements could include the collection of required personal data, proper maintenance of that data in the airport badging system databases, consistency in dates with the information from the hard copy applications, and "cleared" status for employee prior to a grant of unescorted access.

Recommendation #5: Provide Transportation Security Inspectors with real time reports generated from the existing database of all active badge holders for analysis. These reports should include an analysis identifying possible records with data inaccuracies based on factors such as age and duplicate personal identification numbers. The reports should provide the agency with immediate capabilities to effectively monitor and track the clearance process.

TSA Concurs, In Part. While we understand the intent of this recommendation, the capability for real-time requests for badge personnel at any airport does not exist at this time. Currently, TSA requires a monthly submission pursuant to SD 1542-04-8G for airport operators, by airport category. This includes a comprehensive list of badge/media holders along with an audit of their media holdings (not less than 10 percent via random selection every 6 months) during TSA-led comprehensive inspections each year. TSA will consider the feasibility of requiring additional reports.

Recommendation #6: Require airports to conduct a criminal history records check for each badge holder on a recurrent basis to correspond with badge renewal. This will ensure that individuals who have committed disqualifying crimes no longer have access to secured airport areas.

TSA Concurs. As explained in the response to Recommendation #3, TSA is developing a proposed rule intended to improve and standardize the processes and criteria used for almost all of the STAs conducted under TSA's regulations. Among other things, this rulemaking will propose a standard duration for all STAs conducted by TSA, including STAs for airport workers. The standard duration means that all STAs, including airport worker STAs, will expire after a set time. After this set time the individual would need to reapply for his or her STA, and the checks comprising the STA would be repeated, including the criminal history records check. While the rulemaking has not completed coordination, we believe that the Universal Rule initiative will adequately address this recommendation.

Appendix C
Applicant Information Required for Security Threat Assessments

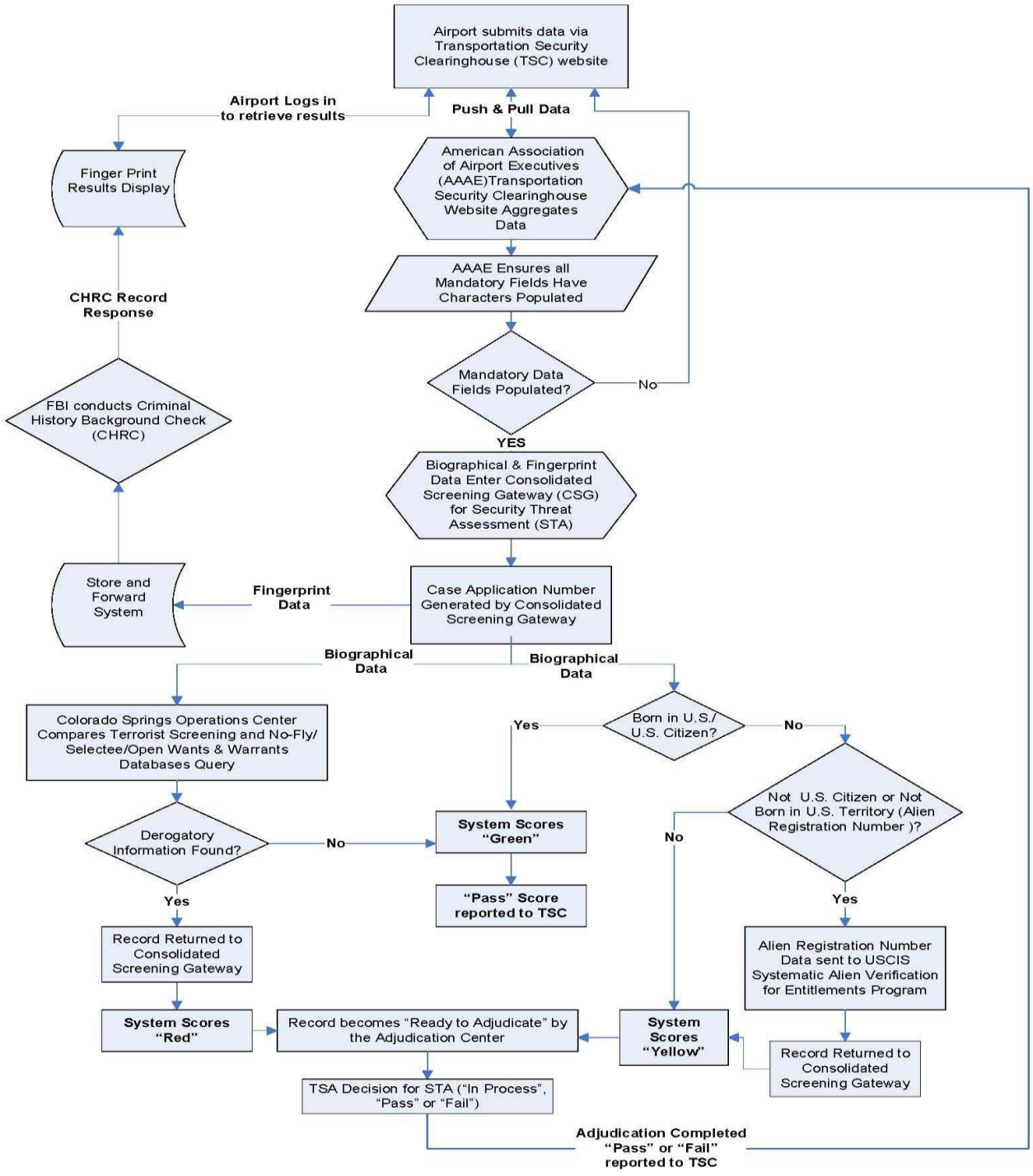
To initiate a security threat assessment, airport operators must submit the following applicant information to TSA:

- ☑ Full legal name
- ☑ Current address
- ☑ Phone number
- ☑ Gender
- ☑ Date of birth, country of birth, citizenship country code
- ☑ Social Security number (optional, but providing it expedites the process)
- ☑ Non-U.S. citizens: Alien registration number and I-94 Form number
- ☑ Nonimmigrant visa holders: Visa control number
- ☑ Numerous items for U.S. citizens born abroad
- ☑ Employer's name
- ☑ Airport code, airport category
- ☑ Identification media information (such as level of access)

To initiate a criminal history records check, airport operators must:

- ☑ Verify the identity of the individual through two forms of identification
- ☑ Collect, control, and process one set of legible and classifiable fingerprints under direct observation of the airport operator or a law enforcement officer.
- ☑ Submit fingerprint data to the FBI for processing

Appendix D
Flowchart of the Vetting Process



-	Total Individuals with Any Omissions or Inaccuracies	Regulatory Omissions or Inaccuracies	STA	Date of Birth	Place of Birth	Name	ARN	Omissions or Inaccuracies in Other Information Used in Vetting	SSN	Passport	Missing or Incomplete Record	Record with Multiple Omissions or Inaccuracies
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

The following identifies the issues which we considered omissions or inaccuracies. The STA, Date of Birth, Place of Birth, Name, and ARN categories were further identified as regulatory discrepancies:

STA: No proof of STA, or badge was issued before an approved STA result was received.
Date of Birth: Date of birth incorrectly entered in electronic system.
Place of Birth: Not contained in supporting documents with a record, or place of birth incorrectly entered in electronic system.
Name: Misspelled first name, last name, or middle initial.
ARN: Incorrect alien registration number in electronic system.

We also considered Social Security and passport numbers as Inaccuracies as these data elements are additional unique identifiers that can assist in the verification of an individual's identity.

SSN: Incorrect Social Security number in electronic system.
Passport: Incorrect passport number in electronic system.
Incomplete Record: Problems with–

- Blank Field: Hardcopy application missing or a specific data field was not filled in, such as passport number, ARN, place of birth, access level, escort privileges, or other identification number.
- Missing Signature: The applicant, airport operator employees, employer, or signatory failed to sign on an appropriate line.
- Missing Printed Name: The applicant, airport operator employees, employer, or signatory failed to print their name on an appropriate line.
- Missing Date: The applicant, airport operator employees, employer, or signatory failed to date the appropriate line.
- Missing Signature and Date: The applicant, airport operator employees, employer, Customs and Border Protection agent, or signatory failed to sign and date on an appropriate line.

Appendix F
List of Disqualifying Crimes

(1) Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. 46306.
(2) Interference with air navigation; 49 U.S.C. 46308.
(3) Improper transportation of a hazardous material; 49 U.S.C. 46312.
(4) Aircraft piracy; 49 U.S.C. 46502.
(5) Interference with flight crew members or flight attendants; 49 U.S.C. 46504.
(6) Commission of certain crimes aboard aircraft in flight; 49 U.S.C. 46506.
(7) Carrying a weapon or explosive aboard aircraft; 49 U.S.C. 46505.
(8) Conveying false information and threats; 49 U.S.C. 46507.
(9) Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. 46502(b).
(10) Lighting violations involving transporting controlled substances; 49 U.S.C. 46315.
(11) Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C. 46314.
(12) Destruction of an aircraft or aircraft facility; 18 U.S.C. 32.
(13) Murder.
(14) Assault with intent to murder.
(15) Espionage.
(16) Sedition.
(17) Kidnapping or hostage taking.
(18) Treason.
(19) Rape or aggravated sexual abuse.
(20) Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.
(21) Extortion.
(22) Armed or felony unarmed robbery.
(23) Distribution of, or intent to distribute, a controlled substance.
(24) Felony arson.
(25) Felony involving a threat.
(26) Felony involving—(i) Willful destruction of property; (ii) Importation or manufacture of a controlled substance; (iii) Burglary; (iv) Theft; (v) Dishonesty, fraud, or misrepresentation; (vi) Possession or distribution of stolen property; (vii) Aggravated assault; (viii) Bribery; or (ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.
(27) Violence at international airports; 18 U.S.C. 37.
(28) Conspiracy or attempt to commit any of the criminal acts listed above.

Appendix G
Major Contributors to this Report

Patrick O'Malley, Director, Transportation Security Division
Sharon Trodden, Audit Manager
Anthony Colache Auditor-in-Charge
Michael Brunelle, Program Analyst
Gregory Crissey, Program Analyst
Ruth Arevalo, Program Analyst
Corneliu Buzesan, Program Analyst
Brandon Landry, Program Analyst
Scott Wrightson, Program Analyst
Mohammad Islam, Statistician
Elizabeth Clark, Independent Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs

Transportation Security Administration

Administrator
OIG Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

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

OIG HOTLINE

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

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

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