

**TSA Could Improve Its
Oversight of Airport
Controls over Access
Media Badges**

(Redacted)





~~SENSITIVE SECURITY INFORMATION~~

DHS OIG HIGHLIGHTS

TSA Could Improve Its Oversight of Airport Controls over Access Media Badges

October 14, 2016

Why We Did This Inspection

In February 2015, national news outlets reported that badges used by individuals working at airports to access nonpublic areas of the airport were missing and could pose a security threat. We sought to determine whether the Transportation Security Administration (TSA) adequately oversees selected badge controls at airports and thus mitigates the risk associated with lost, stolen, and unaccounted for badges.

What We Recommend

We made three recommendations to improve TSA's oversight of airport badge controls.

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

www.oig.dhs.gov

What We Found

Based on its comprehensive and targeted inspections, TSA has asserted that most airports adequately control badges for employees working in nonpublic areas. However, from the results of special inspections conducted by TSA in 2015, as well as our own testing, we conclude that airports do not always properly account for these badges after they are issued. TSA's current inspection practice of relying on information reported by airports about access media badges limits its oversight of badge controls. By testing more controls, which are designed to curtail the number of unaccounted for badges, TSA could strengthen its oversight of airports. Improved oversight by TSA, including encouraging wider use of airports' best practices, would help mitigate the risks to airport security posed by unaccounted for employee badges.

TSA Response

TSA concurred with the recommendations and began taking corrective actions.

OIG-17-04

~~SENSITIVE SECURITY INFORMATION~~

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

October 14, 2016

MEMORANDUM FOR: The Honorable Peter Neffenger
Administrator
Transportation Security Administration

FROM: John Roth *John Roth*
Inspector General

SUBJECT: *TSA Could Improve Its Oversight of Airport Controls over
Access Media Badges – Sensitive Security Information*

For your action is our final report, *TSA Could Improve Its Oversight of Airport Controls over Access Media Badges – Sensitive Security Information*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving TSA's oversight of airport badge controls. Your office concurred with the three recommendations. Based on information provided in your response to the draft report, we consider all three 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. Please send your response or closure request to OIGInspectionsFollowup@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 Anne L. Richards, Assistant Inspector General for Inspections and Evaluations, at (202) 254-4100.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

The Transportation Security Administration (TSA) is responsible for reducing security vulnerabilities and ensuring the safety and free movement of people and commerce in the Nation's transportation systems. As part of this mission, by statute, TSA is to ensure that airports have adequate controls over approving, issuing, and accounting for access media badges.¹

The Code of Federal Regulations (CFR) mandates that all locally regulated airports implement a TSA-approved security program, which TSA refers to as an Airport Security Program (ASP), specifying how an airport will meet CFR requirements.² ASPs contain security measures, including measures to protect the airport against acts of violence, air piracy, and the introduction of explosives, incendiaries, or weapons aboard aircraft; they also contain access media badge control procedures. Airport operators may amend their ASPs by submitting a written request to TSA. TSA may also amend an airport's ASP if it determines that airport safety and public interest require an amendment.

Access Media Badge Issuance and Accountability

Airport operators are responsible for approving and issuing access media badges to airport and government employees, airline personnel, concessionaires, retailers, and contractors who work at the airport. Although they may issue more, airport operators generally issue three types of access media badges to aviation workers³ working in the following nonpublic areas of an airport:

- Sterile Area – often referred to as the terminal, the area where passengers access boarding aircraft. TSA generally controls this area through screening of passengers, carry-on baggage, and aviation workers working in this area.
- Secured Area – the area where passengers, baggage, and cargo are actively loaded or unloaded on a passenger aircraft. Each secured area is a Security Identification Display Area where aviation workers must display their access media badges.

¹ Access media badges, also referred to as Personal Identification System Media, are issued to aviation workers who require access to nonpublic areas of an airport.

² 49 CFR part 1542

³ An aviation worker is an employee, contractor, or representative of an airport, domestic or foreign airline, vendor, concessionaire, tenant, government agency, entity in the air cargo supply chain, or other entity working or operating at an airport.

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



SENSITIVE SECURITY INFORMATION
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Air Operations Area – the area that includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas for use by aircraft.

After issuing access media badges, airport operators must account for all badges through control procedures specified in TSA's security directive and contained in ASPs. To ensure accountability, TSA's security directive requires airport operators to:

- immediately deactivate lost, stolen, and unaccounted for access media badges;⁴
- renew all access media badges at least once every 2 years; and
- complete a comprehensive audit of all airport-issued access media badges at least once every 12 months to verify the employment and operational need for an access media badge for all badge holders. In addition, airport operators must audit [REDACTED] of all badges (randomly selected) every [REDACTED]. If more than 5 percent of all airport-issued, unexpired access media badges for any nonpublic area are lost, stolen, or otherwise unaccounted for, the airport operator must reissue access media badges for that nonpublic area.⁵

TSA, as well as all companies doing business (employers) at an airport, must assign an authorized signatory as the primary point of contact with the airport operator. Authorized signatories must:

- ensure all of the employer's badge holder information is accurate and current;
- sponsor and request access media badges on behalf of employees seeking unescorted access to nonpublic areas;
- inform the airport operator which employees have an operational need for access media badges;
- notify the airport operator when employees report access media badges lost or stolen; and
- notify the airport operator immediately when an employee separates or is terminated.

⁴ According to TSA, badges issued to individuals who are no longer employed at the airport, but which have not been returned to the airport operator, are considered unaccounted for badges; badges returned to the airport operator are no longer considered unaccounted for.

⁵ Security Directive 1542-04-08K, Attachment B, I.B.1
www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

TSA Inspections

Every year, Transportation Security Inspectors (TSI) from TSA's Office of Security Operations conduct either a comprehensive or a targeted inspection. These inspections, conducted in alternating years, assess airports' compliance with TSA's security directives and Federal regulations. Comprehensive inspections focus on determining an airport's compliance with its ASP, applicable security directives, and CFR-mandated operational requirements. These inspections include:

- inspecting the airport operator's badging office documents;
- randomly screening employees and access media badges;
- reviewing the airport operator's annual access media badge audit;
- observing the airport's or airline's random screening for prohibited items;
- testing access and perimeter controls; and
- verifying that recordkeeping for security threat assessments and criminal history record checks meets requirements.

In alternate years, TSIs conduct targeted inspections focused on certain operational requirements. During these abbreviated, risk-based inspections, TSIs may test specific security requirements, including those related to access media badge controls.

TSA's Office of Security Operations also directed compliance field offices to conduct special emphasis inspections (SEI) of airports. These inspections focus on high risk areas and procedures to mitigate the risk of insider threat. SEIs may be conducted any time at TSA's discretion. In 2015, TSA conducted SEIs at 317 U.S. airports.⁶ According to TSA, the SEIs were the result of a review of inspection activity and were focused on access media badge procedures and insider threat.

⁶ *Unaccounted Airport Operator or Airport Approved ID Media for Domestic Airports* (SEI-2015-002)

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

News Reports of Missing Badges

Prior to the 2015 SEIs, in February 2015, national news outlets reported that thousands of access media badges were missing from various U.S. airports. According to one report, an official from the Hartsfield-Jackson Atlanta International Airport said that, over 2 years, more than 1,400 badges were lost or stolen. Some members of Congress expressed concern that these missing badges would allow an unauthorized person access to an airport's secured areas.

Results of Inspection

Based on its comprehensive and targeted inspections, TSA has asserted that most airports adequately control badges for employees working in nonpublic areas. However, from the results of TSA's SEIs conducted in 2015, as well as our own testing, we conclude that airports do not always properly account for access media badges after they are issued to employees. TSA's current inspection practice of relying on information reported by airports about access media badges limits its oversight of badge controls. By testing more controls, which are designed to curtail the number of unaccounted for badges, TSA could strengthen its oversight of airports. Improved oversight by TSA, including encouraging wider use of airports' best practices, would help mitigate the risks to airport security posed by unaccounted for employee badges.

TSA's Reliance on Airports' Self-Reported Information Limits Its Oversight of Controls over Access Media Badge Accountability

TSA based its assertion that airports were properly accounting for access media badges on information reported by airports about annual audits conducted by airport operators, rather than the results of its own testing of badge controls. When TSA tested controls during the 2015 SEIs, it discovered lost, stolen, and unaccounted for badges at some airports that had not been identified during the airports' audits. We tested badge controls at 24 airports and identified discrepancies in the number of active badges, as well as unaccounted for badges. Through the 2015 SEIs, TSA also realized that some airport operators and TSA personnel were misinterpreting its guidance on how to determine the acceptable percentage of lost, stolen, or unaccounted for badges; as a result, some airports believed to be in compliance with TSA's security directive had actually exceeded the 5 percent threshold. Although TSA

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



SENSITIVE SECURITY INFORMATION
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

later attempted to clarify its guidance, we found that some airports continued to misunderstand the policy.

Access Media Badge Audits

According to TSA's security directive, to ensure airports properly account for all access media badges that have been issued, airport operators are required to audit all these badges at least once every 12 months. [REDACTED]

[REDACTED] The security directive requires employees, as well as employers' authorized signatories, to immediately notify airport operators about badges that are lost, stolen, or unaccounted for. Upon notification, airport operators must immediately deactivate these badges.

During comprehensive and targeted inspections, TSIs do not validate the results airport operators provide from their annual audits of badges. For the part of the inspection dedicated to access media badges, TSIs are required only to confirm that airport operators have conducted the annual audits of their badges. Thus, TSIs simply check to make sure the annual audit has been completed on time and that the appropriate airport official has signed off on the results.

In 2015, TSA headquarters directed TSIs conducting SEIs at 317 airports to test access media badge controls. TSA headquarters also sent guidance reminding TSIs and TSA airport personnel how to properly determine the 5 percent threshold for lost, stolen, and unaccounted for badges. During the SEIs, TSIs first confirmed that the required annual audits of all badges and semiannual audits of [REDACTED] of badges had been completed. In addition, at each airport, [REDACTED]

[REDACTED] As a result of these tests, TSA discovered that [REDACTED] airports exceeded the 5 percent threshold of lost, stolen, and unaccounted for access media badges in at least one nonpublic area.⁷ These badges had not been identified through TSA's previous

⁷ Because some airports exceeded the threshold in more than one area, in total, 33 areas exceeded the threshold.

SENSITIVE SECURITY INFORMATION



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

comprehensive or targeted inspections or through the airports' audits. At some airports, these discrepancies were resolved when employers found and returned inactive badges to the airport operator, [REDACTED] airports were required to rebadge all employees in the affected areas.

During our reviews of 24 airports, we conducted a test that showed [REDACTED] of the 24 airports ([REDACTED] percent) did not have accurate information about active access media badges. At each airport, we randomly selected three employers and compared their active employee rosters to the airport operator's list of active access media badges. [REDACTED] of the 24 airport operators had inaccurate lists of active badges. For example, at four different airports:

- The names of 17 employees who no longer worked for an employer and, therefore, whose badges should have been deactivated, were on the airport's list of active access media badges.
- The name of an employee who had been terminated in November 2014 was on the airport operator's active badge list in September 2015.
- The names of three employees who had resigned from one employer were still on the airport operator's active badge list.
- An employer had terminated an employee in May 2015, but the airport operator was not aware of the termination until we brought it to operator's attention in September 2015.

Based on our test results, these [REDACTED] had to deactivate a total of 62 access media badges that airport operators had incorrectly listed as active. All of these badges belonged to individuals who were no longer employed, which the employers had not immediately reported to airport operators. In some cases, the employers had collected the badges but failed to promptly notify and return the badges to the airport operator, as required by the TSA security directive. In other cases, the employers had neither collected the badges of the former employees nor notified the airport operator; therefore, those badges could have been used to access a nonpublic area of the airport. Based on our test results, TSA took enforcement action, such as a warning letter or monetary penalty, against the employers who had not promptly notified the airport operators.

Five Percent Threshold

During its 2015 SEIs, TSA also discovered that some airport operators and local TSA airport personnel were interpreting guidance on the 5 percent

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

threshold incorrectly. According to TSA's security directive, no more than 5 percent of all badges in each nonpublic (sterile, secured, and airport operations) area of the airport may be lost, stolen, or unaccounted for. Rather than determining the percentage in each of the three areas separately, some airports were aggregating the lost, stolen, or unaccounted for badges as a percentage of all access media badges issued. One airport was excluding sterile area badges from the percentage determination. As a result, the total percentage may have been under the 5 percent threshold, even if the percentage in one or two areas exceeded 5 percent. Therefore, some airports thought to be in compliance with the security directive may have actually exceeded the authorized percentage in one or more areas.

Because of these errors in interpreting guidance, on June 8, 2015, and June 30, 2015, TSA headquarters issued two memoranda to all Assistant Federal Security Directors to reiterate and clarify access media badge regulations in its security directive. Although TSA sought to clarify the 5 percent rule, [REDACTED] of the 24 airports we reviewed after the memoranda were issued, local TSA airport personnel and airport operators continued to have difficulty understanding the rule and were interpreting it differently. For example, at one airport, both the airport operator and local TSA personnel considered the sterile area a public area and, therefore, did not include it when determining the percentage of lost, stolen, or unaccounted for badges. At another airport, the operator continued to struggle with the 5 percent threshold and wanted TSA to clarify how to properly calculate the percentage of lost, stolen, and unaccounted for badges.

We recommend that the TSA Administrator:

Recommendation 1: Direct TSA personnel to conduct additional tests of access media badge controls during comprehensive and targeted inspections of U.S. airports.

Recommendation 2: Issue guidance to U.S. airports clearly explaining how to determine whether an airport's lost, stolen, and unaccounted for access media badges are exceeding the 5 percent threshold.

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



SENSITIVE SECURITY INFORMATION
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

TSA Could Help Airport Operators Improve Badge Accountability by Sharing and Encouraging Best Practices

Of the 24 airports we reviewed, [REDACTED] had established quality assurance procedures exceeding TSA's requirements to mitigate the risks of lost, stolen, and unaccounted for access media badges. These airports have established best practices, including conducting "reverse audits," renewing certain types of access media badges more often than the required 2 years, and offering annual refresher training for current access media badge holders. By sharing these practices with airport operators and encouraging use of them when feasible, TSA could improve its oversight and help ensure better accountability of access media badges.

Conducting Reverse Audits

Some of the 24 airports we reviewed adopted the annual audit guidance in TSA's security directive, in which an airport operator [REDACTED]. However, the results of TSA's 2015 SEIs and our test results showed this is not always the most effective way to ensure the accountability of access media badges. To improve accountability, some airports we reviewed have reversed this process. That is, during an audit, the airport operator requests employers' current employee rosters and compares them against its own lists of active badges, [REDACTED]. If the airport operator finds its list contains active badges for employees not on an employer's roster, the airport can immediately deactivate the badges. Not all airports we visited used this method consistently. For example, one airport operator only used the method with employers that did not comply with the airport's accountability requirements; another airport operator used it periodically.

Renewing Access Media Badges More Often Than Every 2 Years

TSA's security directive requires airport operators to renew access media badges at least once every 2 years, but some airports we reviewed renew badges more often. For example, [REDACTED] the 24 airports we reviewed renew all access media badges annually. [REDACTED]

SENSITIVE SECURITY INFORMATION

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



SENSITIVE SECURITY INFORMATION
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security



Annual Refresher Access Media Badge Training

TSA requires airport operators to develop and implement a TSA-approved curriculum to train individuals when they apply for access media badges. When training is complete, employees are tested; airport operators issue access media badges to employees who complete the training and pass the test. As part of their comprehensive inspections, TSIs ensure that airport operators are providing initial training and that it meets all requirements. TSIs also verify that individuals have successfully completed the initial training before they are issued access media badges.

Although the initial training meets regulatory requirements, TSA does not have a policy regarding refresher training for badge holders. Nevertheless, some airports have established annual refresher training for employees to ensure they are aware of their duties and responsibilities as badge holders. For example, of the 24 airports we reviewed, 11 conduct annual refresher training for all badge holders, and 3 have established biennial refresher training. One airport recognized the importance and advantage of providing annual recurring training and decided to implement such training for all of its badge holders by the end of 2015.

Recommendation 3: We recommend that TSA share with airport operators the best practices some airports use to mitigate the risks of lost, stolen, and unaccounted for access media badges and encourage airport operators to use these practices when feasible.

Conclusion

Unless airport operators and employers properly account for the access media badges of individuals no longer employed at the airport, as well as lost and stolen badges, there is a risk that former aviation workers or unauthorized individuals can access nonpublic areas. Stronger oversight by TSA will help ensure better accountability of access media badges by both the airport operators and employers, and mitigate this risk.

SENSITIVE SECURITY INFORMATION



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Management Comments and OIG Analysis

TSA concurred with our recommendations and provided comments to the draft report. A summary of TSA's management comments and our analysis follows. We have included a copy of TSA's management comments in their entirety in appendix A. TSA also provided technical comments to our report, which we incorporated, as appropriate.

Recommendation #1: TSA concurred. TSA is developing inspection protocols and planning additional tests and inspections of access media badge controls in fiscal year 2017. The testing will include badge deactivation tests, airport badging office audits of badges, and other related areas. To combat insider threat, TSA will also expand and enhance its assessment, inspection, and testing, including expanding its access media badge-related tests and inspections.

OIG Analysis: TSA's planned actions are responsive to this recommendation. This recommendation is resolved, but will remain open until TSA completes the first round of inspections in the first quarter of FY 2017. TSA should provide the inspection protocols and results of the first round of inspections when they are completed.

Recommendation #2: TSA concurred. TSA will clarify how to determine whether an airport's lost, stolen, and unaccounted for access media badges exceed the 5 percent threshold and update the security directive. TSA estimates it will complete these corrective actions by December 31, 2016.

OIG Analysis: TSA's corrective actions are responsive to the recommendation. This recommendation is resolved, but will remain open until TSA provides documentation to support corrective actions taken, including a copy of the security directive containing the security requirements for badge audit requirements.

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation #3: TSA concurred. TSA recognizes the benefits of sharing best practices and has already begun to share Aviation Security Advisory Committee recommendations and best practices related to badge audits with regulated airports. In addition, TSA has shared the results of effective measures identified through self-vulnerability assessments. TSA plans to continue to review access media badge program best practices and develop a best practice document by December 31, 2016.

OIG Analysis: TSA's corrective action is responsive to the recommendation. This recommendation is resolved, but will remain open until TSA releases the best practice document.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-206) by amendment to the *Inspector General Act of 1978*.

We conducted this inspection to determine whether TSA has adequate oversight of selected access media badge controls at airports by testing selected controls designed to mitigate the risks associated with lost, stolen, or unaccounted for access media badges.

We reviewed applicable Federal laws, directives, and regulations, the TSA ASP and 49 CFR 1542 *Implementation Guidance*, TSA Security Directive 1542-04-08 series, and various ASPs. In addition, we reviewed prior OIG reports and U.S. Government Accountability Office reports on TSA's oversight of airport access media badges.

We interviewed officials from TSA's Office of Security Operations, airport Federal Security Directors and Assistant Federal Security Directors, TSIs, and randomly selected aviation workers. We also interviewed airport operator personnel responsible for the access media badge program. We toured airport facilities, with a focus on entry and exits points that airport personnel with access media badges use to access secured and sterile areas.

We conducted several tests and observed TSA's and airports' daily operations. At each of the 24 airports we reviewed, to determine whether there were discrepancies, we compared airport operators' lists of active access media badges to employee rosters of three randomly selected employers.

www.oig.dhs.gov

11

OIG-17-04

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



SENSITIVE SECURITY INFORMATION
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We reviewed and conducted tests onsite at 24 airports:



We selected these airports based on size, daily volume of airline travelers, and geographical location.

We conducted this inspection between April and November 2015 under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

SENSITIVE SECURITY INFORMATION

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A
TSA Comments to the Draft Report

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



**Transportation
Security
Administration**

SEP 27 2016

INFORMATION

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

FROM: Huban A. Gowadia, Ph.D. *Huban Gowadia*
Deputy Administrator *27 SEPT 16*

SUBJECT: Response to Draft Report, *TSA Could Improve its Oversight of Airport Controls over Access Media Badges*, OIG Project No. 15-099-ISP-TSA

This memorandum constitutes the Transportation Security Administration's (TSA) response to the U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) draft report, *TSA Could Improve its Oversight of Airport Controls over Access Media Badges*, OIG Project No. 15-099-ISP-TSA, August 2016.

Regulation and inspection oversight of airport operators are important to TSA's mission. TSA is grateful for the OIG's efforts to examine and help improve our oversight of airport operators. TSA appreciates the OIG's recognition of the critical role of Transportation Security Inspectors (TSIs) in the Office of Security Operations Compliance Programs Division in performing regulatory compliance inspections and tests of airport operator ID media processes and audits.

While the current ID media oversight and auditing program effectively mitigates the risk of lost, stolen, or otherwise unaccounted for badges, the OIG's recommendations will help improve TSA's oversight and auditing program. The OIG's recommendations mirror enhancements achieved in this program in the last two years. TSA enhancements include additional auditing program testing and inspections, both conducted by TSA's Office of Security Operations Compliance Programs Division, and sharing of audit-related best practices by TSA's Offices of Security Policy and Industry Engagement and Security Operations.

TSA will continue to work with the OIG and the aviation industry to improve ID media practices and oversight. TSA uses local and national stakeholder engagement to share best practices. This sharing occurs after Compliance Security Enhancement Through Testing (COMSETT) cycles and after all other TSI engagements with stakeholders, including assessments, inspections, tests, and outreaches. At a national level, TSA engages with stakeholder associations, including

~~SENSITIVE SECURITY INFORMATION~~

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

2

sharing COMSETT and SEI results, and working with industry on in-depth security reviews of Security Directives, best practices, and TSI findings.

TSA concurs with all three OIG recommendations related to ID media oversight. We are please to note that significant progress has already been made toward implementing the OIG recommendations. We are conducting additional tests and special emphasis inspections; we are reissuing guidance to more clearly explain and define counting methodologies for badge reissuance; and we will continue to share best practices.

TSA values the OIG's recognition of our partnership with airport operators and other airport stakeholders. TSA looks forward to working with industry, the OIG, airport operators, airlines, and other stakeholders to ensure compliance with current ID media security requirements, share best practices, and mitigate any vulnerabilities.

Attachment:
TSA Response to OIG Recommendations

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

Response to OIG Draft Report

TSA Could Improve its Oversight of Airport Controls over Access Media Badges
OIG Project No. 15-099-ISP-TSA

Recommendation 1: Direct TSA personnel to conduct additional tests of access media badge controls during comprehensive and targeted inspections of U.S. airports.

TSA concurs. TSA's Office of Security Operations (OSO) plans to conduct additional tests and inspections in Fiscal Year 2017 (FY 2017) related to identification (ID) media controls, including badge deactivation tests, airport badging office audits of ID media, and related areas. These tests will include Special Emphasis Inspections (SEIs) and comprehensive and targeted inspections of regulated airports with secured and sterile areas, and of airlines with Exclusive Area Agreements (EAAs). In a risk-based approach to an ID media system with more than 1.3 million badges nationally, TSA will be expanding and enhancing its assessment, inspection, and testing efforts to combat the insider threat, including expanding its ID media-related tests and inspections, analyzing the results for any ongoing vulnerabilities, and partnering with local airport operators and other industry stakeholders to collaboratively mitigate these vulnerabilities. Our latest round of Compliance Security Enhancement Through Testing (COMSETT) testing indicated that airport operators effectively deactivate a significantly high percent of ID media that is reported lost, stolen, or otherwise unaccounted for. While this is a very high pass rate, TSA plans to continue testing and inspecting the entire area of insider threat mitigation measures, including perimeter and access control security measures and the ID media program.

SEIs will be conducted in the first and fourth quarters of FY 2017. The inspection protocols are being developed and will be ready for dissemination by October 1, 2016. Inspectors will focus on doing the following:

1. Test airports and EAAs to ensure that badges reported as lost or stolen, and badges of employees whose employment has been terminated are appropriately deactivated.
2. Conduct a reverse audit of two tenants and one domestic air carrier or one foreign aircraft operator's active badges.
3. Inspect the airports auditing procedures.

TSA will complete the first round of inspection results in the first quarter of FY 2017. TSA will conduct this additional oversight and auditing twice a year.

Recommendation 2: Issue guidance to U.S. airports clearly explaining how to determine whether an airport's lost, stolen, and unaccounted for access media badges are exceeding the five percent threshold.

TSA concurs. TSA's Office of Security Policy and Industry Engagement (OSPIE) will provide clarification for how to determine whether an airport's lost, stolen, and unaccounted for access media exceed the five percent threshold. TSA will renew the current Security Directive (SD) containing the security requirements for badge audit requirements by December 31, 2016.

~~SENSITIVE SECURITY INFORMATION~~

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

2

Recommendation 3: We recommend that TSA share with airport operators the best practices some airports use to mitigate the risks of lost, stolen, and unaccounted for access media badges and encourage airport operators to use these practices when feasible.

TSA concurs. While this recommendation has already been partially implemented, OSPIE and OSO will work collaboratively with industry to expand our best practices sharing in FY 2017. In FY 2016, TSA shared with regulated airports via the Homeland Security Information Network all of the Aviation Security Advisory Committee recommendations and best practices related to badge audits. TSA also reviewed the results of the self-vulnerability assessments related to perimeter and access control security measures, including the ID media audit and implementation program performed by regulated airports and airlines with EAAs. After its review, TSA shared effective measures, including measures related to badge audits, with these industry stakeholders. In FY 2017, TSA plans to continue to review ID media program best practices and implementation practices, and provide additional best practices guidance in this area. Specifically, we will review and consider sharing those best practices identified by the OIG related to the ID media oversight and audit program.

TSA will release a best practice document during the first quarter of FY 2017.

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix B
Office of Inspections and Evaluations Major Contributors to This Report

John D. Shiffer, Chief Inspector
Angela Garvin, Chief Inspector
Wayne Ekblad, Supervisory Inspector
Inez Jordan, Supervisory Inspector
Natalie Fussell Enclade, Policy Advisor
Michael Brooks, Senior Inspector,
Raymond Motlasz, Investigator
Adam Brown, Senior Inspector
Connie Tan, Senior Inspector
Marissa Weinshel, Program Analyst
Glenn Stewart, Inspector
Brianna Cumana, Inspector
Kimberly Crabbe, Inspector
Robin Goodrich, Administrative Officer
Kelly Herberger, Communications Analyst
Renita L. Hunter-Caracciolo, Independent Reference Reviewer

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix C

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
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
DHS Component Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

~~SENSITIVE SECURITY INFORMATION~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

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