

DEPARTMENT OF HOMELAND SECURITY Office of Inspector General

Audit of Access to Airport Secured Areas (Unclassified Summary)





**Homeland
Security**

March 15, 2007

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 airport operators and air carriers in preventing access by unauthorized persons to defined secured areas of the airport. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations in the report have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that 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

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

OIG

*Department of Homeland Security
Office of Inspector General*

Background

Airport operators and aircraft operators each have responsibilities under the Code of Federal Regulations, and their respective approved security programs, to meet certain security requirements. Among these requirements is the responsibility to prevent access by unauthorized persons to defined secured areas of the airport. Transportation Security Administration (TSA) regulations require personnel who enter the Security Identification Display Area (SIDA) and other secured areas of the airport to have an airport issued or approved SIDA badge properly displayed on their person or to be under escort. No airport operator may grant unescorted access to the secured area or SIDA to any individual unless that person has successfully completed training according to a TSA approved curriculum specified in the airport security program. The curriculum must include: (1) the unescorted access authority of the individual to enter and be present in various areas of the airport; (2) the control, use, and display of airport approved access and identification media; and (3) escort and challenge procedures, and the law enforcement support for these procedures.

We performed access control testing at 14 domestic airports of various sizes nationwide. Altogether, our four-person team conducted more than 600 access control tests.

Results of Audit

We identified various weaknesses in TSA's procedures to prevent unauthorized individuals from access to secured airport areas. We made several recommendations that, if implemented by TSA, airport operators, and air carriers, can enhance the overall effectiveness of controls that limit access to airport secured areas.

TSA's Response

TSA said that all of our recommendations highlight areas of interest to TSA. TSA provided an extensive response to our draft report, describing actions that it has already taken to address each of our recommendations.

TSA fully concurred with all but one of our recommendations, which is discussed here. Although TSA also concurred with our recommendation that the TSA Assistant Secretary deploy available technology to detect explosives on passengers at airports nationwide for continuous random screening of passengers in addition to use on selectees, it offered extensive explanation of the significant efforts that have been underway at TSA for more than 18 months to improve the performance of Transportation Security Officers (TSOs).

The following summarizes TSA's response to our draft report. We did not validate this information because TSA provided it after completion of our review.

TSA approved immediate, mid-term, and long-term steps to counter the threat in August 2005. The short and mid-term strategies would have to yield IED solutions that were people-based, not equipment or technology-based. Accordingly, TSA's strategy is to rely on the TSOs to enhance checkpoint detection capability. A key part of this reliance on the TSOs was to train, equip, and empower them; trust their judgment, and guide them away from a script-based system of security and into a model where their judgment, discretion, and experience mattered.

Also, TSA took immediate steps to build on TSO performance by instituting randomness as a cornerstone of its security posture. For example, TSA recently implemented a passenger checkpoint enhancement called Unpredictable Screening Procedures. This change provides a structure for random sampling of carry-on bags with Explosives Trace Detection equipment.

TSA also implemented the Aviation Direct Access Screening Program (ADASP). ADASP allows TSOs to randomly screen airport and airline employees, their accessible property, and their vehicles as they enter airport restricted areas other than through a screening checkpoint.

In addition, TSA implemented a behavior recognition program called Screening Passengers by Observation Techniques (SPOT), which focuses on behavior observation and analysis. SPOT is currently operational at many of our Nation's airports, and TSA is executing an aggressive plan to implement the program at all major airports by the end of the year.

Also, TSA is implementing IED Checkpoint Screening Drills. These drills will expose TSOs to simulated threat items in a regular and standardized way through hands-on training at the checkpoint. As part of this program, TSOs will also be routinely exposed to simulated threat items without warning. These exercises will be conducted daily, and, once fully implemented, TSA

expects more than 50,000 drills to be conducted at airports around the country each month.

Finally, TSA's covert testing program includes screening checkpoint testing, checked baggage testing, and access testing of restricted areas of commercial airports. These tests employ a variety of methods of inserting prohibited items into the sterile area that mimic real-world possibilities based on the most current intelligence available. In its testing, TSA continues to adapt procedures to accommodate the deployment of new security screening technologies and procedures.

As part of its long range strategy, TSA is actively pursuing security initiatives that it characterizes as the "Checkpoint of the Future." This includes developing technologies that, when fielded, will reduce the vulnerabilities that we identified in our report. These technologies include backscatter and multi-view x-rays at the checkpoint for both passengers and their carry-on baggage.

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, 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 misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.