Department of Homeland Security
Office of Inspector General

TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening (Revised for Public Disclosure)

(Redacted)

OIG-09-05

October 2008

Office of Inspector General

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

Homeland Security

October 28, 2008

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.

In response to a congressional request from U.S. Representative Bennie G. Thompson, Chairman of the House Committee on Homeland Security, and Representative Ric Keller, our report addresses the strengths and weaknesses of the Transportation Security Administration's oversight of security-screening procedures for airport employees with access to secure areas of an 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 herein 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.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendixes

Abbreviations

ADASP	Aviation Direct Access Screening Program
DHS	Department of Homeland Security
FAM	Federal Air Marshal
MCO	Orlando International Airport
OIG	Office of Inspector General
SIDA	Secure Identification Display Area
SJU	Luis Munoz Marin International Airport, San Juan, Puerto Rico
TSA	Transportation Security Administration
VIPR	Visible Inter-Modal Protection and Response

Executive Summary

At the request of Representative Bennie G. Thompson, Chairman of the House Committee on Homeland Security, and Representative Ric Keller, we reviewed the events surrounding a March 5, 2007, security breach at the Orlando International Airport in Florida. The breach involved two Comair Airline employees who smuggled 14 firearms and 8 pounds of marijuana onboard a Delta Airlines commercial airplane bound for San Juan, Puerto Rico. Specifically, we assessed (1) the actions, events, and communication surrounding the incident; (2) the Transportation Security Administration's current oversight of airport employees; and (3) the feasibility of 100% airport employee screening for individuals accessing an aircraft or the secure areas of an airport.

The Transportation Security Administration has made improvements to address vulnerabilities associated with the "insider threat" highlighted by the March 5, 2007, incident. These improvements include the widespread implementation of two random and deterrent-based screening programs: the Aviation Direct Access Screening Program and the Visible Intermodal Protection and Response Program. In addition, the Transportation Security Administration started conducting Security Threat Assessments of airport employees to assess whether workers have ties to terrorism or are in violation of immigration and admissibility laws.

Even with these improvements, the Orlando incident revealed the need for additional changes. Specifically, the Transportation Security Administration needs improvements in its ability to obtain and maintain situational awareness of incidents, as well as updating its regulatory framework that governs airport employee conduct. These changes are necessary before a decision is made about implementing 100% employee screening.

We are making six recommendations to assist the Transportation Security Administration in improving the overall security posture at airports. In response to our report, the Transportation Security Administration has proposed plans and actions that, once implemented, will reduce a number of the deficiencies we identified. The Transportation Security Administration concurred with all six recommendations.

Background

On March 5, 2007, two Comair Airline employees from Orlando International Airport (MCO) in Florida successfully smuggled 14 firearms and 8 pounds of marijuana aboard Delta Airlines Flight #933 bound for Luis Munoz Marin International Airport (SJU) in San Juan, Puerto Rico. Both individuals were later arrested; one in Puerto Rico upon the flight's arrival, and one in Orlando the following day.

On March 8, 2007, Representative Ric Keller requested that we review the Transportation Security Administration's (TSA) role in the events surrounding this incident, to determine whether the absence of specific screening policies for airport employees facilitated this security breach. On March 26, 2007, Representative Bennie G. Thompson, Chairman of the House Committee on Homeland Security, contacted us with a similar request. After considering both requests, we agreed to review the incident, as well as assess the security-screening procedures for non-TSA employees working at federalized airports nationwide.

During subsequent discussions with congressional staff, we agreed to focus on three questions:

- Did TSA policies cause MCO to be susceptible to security breaches, particularly involving the introduction of prohibited items into any secure areas of the airport?

- What is the overall effectiveness of TSA's oversight of airport employees?

- What is the feasibility of implementing 100% airport employee screening for individuals accessing an aircraft or the secure areas of an airport?

Currently, Congress is pursuing the 100% airport employee screening issue. In March 2007, H.R. 1413 was introduced by Representative Nita Lowey. This bill calls for TSA to implement a pilot program to screen all airport workers with unescorted access privileges to secure areas at seven airports. In April 2007, a similar bill, S. 1095, was introduced by Senator Charles Schumer. This bill calls for TSA to screen all individuals who have access to the secure areas of airports. This would include airport employees, commercial airline carrier employees, contractors, and vendors. Neither bill was enacted during our fieldwork.

On December, 26, 2007, the President signed the *Consolidated Appropriations Act of 2008*, which mandates TSA evaluate 100%

employee screening at three airports and assess alternative employee screening measures at four other airports. Congress provided TSA $15 million for this pilot program, which was scheduled to run from May 2008 through July 2008.

The three airports participating in the 100% employee screening pilot program were Boston Logan International Airport in Massachusetts, Craven Regional Airport in North Carolina, and Jacksonville International Airport in Florida. The four airports piloting alternative screening measures were Denver International Airport in Colorado, Kansas City International Airport in Missouri, Mahlon Sweet Field Airport and Southwest Oregon Regional Airport in Eugene and North Bend, Oregon respectively.

TSA's Current Oversight and Screening of Non-TSA Airport Employees

TSA has more than 1,200 Transportation Security Inspectors who conduct oversight by inspecting airport, airline, and cargo security operations for compliance with applicable regulations. These inspections are scheduled, conducted randomly, and may include one or all of the security elements required by TSA.

TSA's oversight of non-TSA airport employees covers a number of different areas, including an airport's security program, its badging process, and "challenge" program. Since March 2007, TSA has also developed three additional security programs that focus on airport employee screening. The Aviation Direct Access Screening Program (ADASP) is a random and deterrence-based program; and the Visible Intermodal Protection and Response (VIPR) Program, is a TSA response capability that may be random as a deterrent, or may be targeted. The third program is TSA's Security Threat Assessment vetting.

Airport Security Programs and Related Employee Oversight Elements

Title 49 USC 1542; Airport Security, requires that each airport serving domestic and foreign commercial air carriers have an airport security program. This program must provide for the safety and security of persons and property against acts of criminal violence, aircraft piracy, and the introduction of unauthorized weapons, explosives, or incendiaries onto an aircraft.[1] Of the 21

[1] 49 CFR § 1542.101.

elements required of all airport security plans, 3 directly relate to the oversight of airport employees   the certification of access control systems, criminal history records checks, and the use of personnel identification systems.[2]

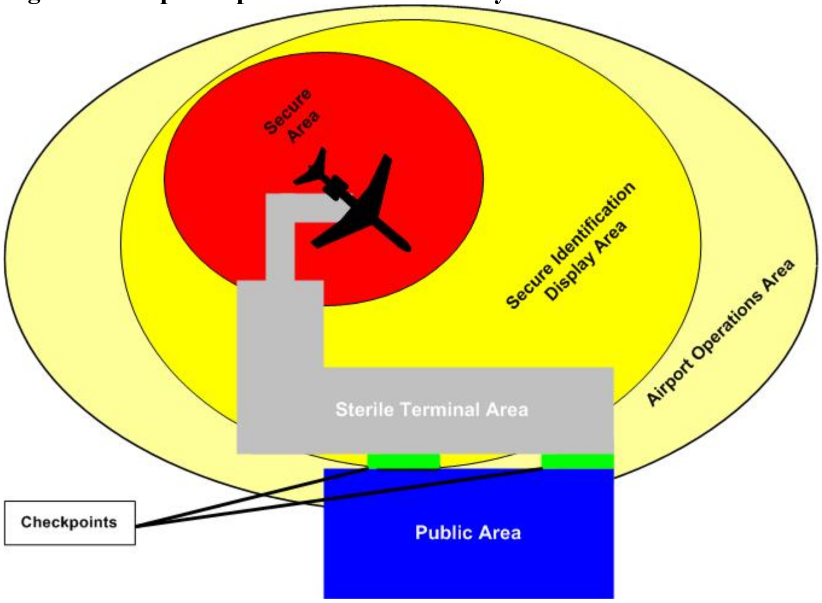
Certification of Access Control Systems

An airport's access control system is required to ensure that only those individuals authorized to have unescorted access into the secured areas are able to gain entry. For those not authorized unescorted access, the airport operator must also establish procedures for escorting individuals in secured areas of the airport. These requirements ensure escorted individuals are continuously accompanied or closely monitored while in secured areas.[3]

An access control system must limit access from the public area to the secure area of an airport. The public areas are the portions of an airport such as parking facilities, airline ticketing, and baggage claim, where access control or screening is not required. The airport operations area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas for use by aircraft. The secure area is the portion of an airport as specified in the Airport Security Plan, where aircraft operators and their contractors enplane and deplane passengers and sort and load baggage. Within the secure area is the sterile area, also a portion of an airport specified in the Airport Security Plan, where individuals have access to boarding aircraft and their property must be screened prior to entering. At many airports, the entire secure area is also defined as a sterile area. Figure 1 illustrates the relationship between the airport operating areas.

[2] 49 CFR § 1542.103.
[3] 49 CFR § 1542.211.

Figure 1: Airport Operations Area Security Distinctions



Criminal History Records Check and Security Threat Assessment

To become eligible for unescorted access into the secured area, an individual must be subjected to a fingerprint-based criminal history records check and the Security Threat Assessment.[4] For the criminal history records check, TSA works with the American Association of Airport Executives, which is responsible for collecting this information from airports and providing it to TSA. TSA then forwards this information to the Federal Bureau of Investigation for processing, and the bureau posts the results to a secure, password-protected website. Airport and airline personnel security officers can then review the information and determine whether an individual can be granted access based on a list of disqualifying criminal offenses. The results are also provided to TSA. A full list of the disqualifying crimes is in Appendix C.

TSA also determined that, in addition to a criminal history records check, there was a need to have additional threat information regarding individuals who applied for or are granted unescorted access at airports. Effective October 1, 2007, TSA mandated that all airport employees would need a TSA-adjudicated Security Threat Assessment before airport operators could issue any type of personnel identification media. This identification, also known as a Secure Identification Display Area (SIDA) badge, is frequently

[4] 49 CFR § 1542.209.

used for unescorted access to the secure areas of an airport.[5] The Security Threat Assessment is a TSA-initiated, name-based check that processes individual names through criminal, terrorist, immigration, and admissibility-related databases. Some of the databases used in conducting the Security Threat Assessment include:

- The Terrorist Screening Database, which contains information about known or suspected terrorists;
- The No-Fly List, which contains the names of people who are not permitted to board a commercial aircraft for travel in the United States; and
- The Selectee List, which is a security measure in the United States that selects passengers for additional screening or secondary inspections.

TSA officials said it conducts Security Threat Assessments on all new airport employees and vets current employees on a perpetual basis. The perpetual vetting will allow for a comparison of new threat information against the names of existing airport employees to account for any derogatory developments.

Use of Personnel Identification Systems

To use an access control system, an individual must successfully complete the criminal history records check and the Security Threat Assessment, and obtain a SIDA badge for unescorted access to the secure areas of an airport.

Guidelines for SIDA badge systems are described in 49 CFR 1542.211. A SIDA badge must convey a full-face image, full name, employer, and identification number of the individual to whom it is issued. The badge must also be displayed on the outermost garment above the waist level. There must also be procedures to ensure accountability of the badges, including retrieving expired badges, reporting lost or stolen badges, and securing unissued badge stock and supplies.

The personnel media system must be audited at least once a year to ensure the integrity and accountability of all identification media.

[5] Security Directive, SD 1542-04-08E, Security Threat Assessment and Reporting Requirements for Individuals with Any Form of Airport Personnel Identification Media.

Also, as specified in the airport security program pursuant to TSA's Complete Airport Security Program Guide, an airport is required to revalidate or reissue SIDA badges when 5% of all issued, unexpired, identification media are lost, stolen, or otherwise unaccounted.[6] When it is determined that 5% of the SIDA badges are unaccounted, the airport must issue new identification media to all authorized persons or revalidate its current SIDA badges. The new or revalidated SIDA badges must be visually distinct from the media being replaced.

In addition, the air carriers and airport tenants who receive identification media must provide immediate notification to the airport operator when an individual's access authority is revoked, limited, or the SIDA badge is lost or stolen. When an individual is terminated, the access media must be retrieved and returned to the airport operator.

Finally, each airport is also required to establish and implement a challenge program.[7] This program requires each SIDA badge holder to confront any individual who has accessed the secured areas and is not displaying a SIDA badge that authorizes the individual to be present in the area.

Additional TSA Security Measures for Airport Employee Oversight

TSA also has developed two additional security programs that focus on airport employee screening. On March 9, 2007, TSA began conducting ADASP operations nationally, on a mandatory basis. This program was designed to conduct random screening operations inside the secure area in an airport, thus providing an additional layer of security at airports. Under this program, Transportation Security Officers can screen TSA, airline and airport employees, as well as passengers and their accessible property. These officers also can inspect vehicles entering an airport operations area. ADASP operations consist of five screening processes:

- Verification of a SIDA badge within the secure area;
- Screening individuals and their accessible property at a boarding gate;
- Aircraft inspection;

[6] Complete Airport Security Program Guide For Category X – III Airports. May 10, 2006.
[7] 49 CFR § 1542.211(d).

- Explosive Trace Detection sampling of accessible property or aircraft; and
- Cargo screening.

In June 2007, TSA also began conducting VIPR operations within the aviation environment. Prior to this time, VIPR operations had been conducted only in modes of transportation outside of the aviation environment. A VIPR team works with local security and law enforcement officials to supplement existing security resources by providing additional deterrence and detection capabilities, while introducing an element of unpredictability into transportation security. These operations are intended to disrupt potential terrorist planning activities. Depending on operational needs, teams can be formed with resources from TSA's Transportation Security Officers, Transportation Security Inspectors, Bomb Appraisal Officers, Federal Air Marshals (FAM), and Behavior Detection Officers. In addition to TSA resources, other Department of Homeland Security (DHS) components, such as U.S. Immigration and Customs Enforcement Special Agents, U.S. Customs and Border Protection Officers, U.S. Coast Guard personnel, and explosives-detection canine teams are used to form VIPR operation teams.

Results of Review

TSA policies and procedures did not cause the March 5, 2007, security breach at MCO because there were no specific airport employee screening mandates in place at that time. However, the breach highlights need for such policies and procedures to reduce the vulnerabilities that were exposed. In addition, TSA's handling of this incident raises questions about TSA's ability to obtain and maintain situational awareness of the incident and the regulatory framework that governs the conduct of employees working at an airport. While the insider threat which includes any current or former employee who has, or had, authorized access or knowledge about an organization's exploitable internal workings remains a concern throughout the aviation community, 100% airport employee screening may not have prevented the March 5, 2007, incident at MCO. Before a decision is made whether to implement 100% employee screening, changes are necessary as to how TSA conducts its oversight of non-TSA airport employees.

Security Breach at the Orlando Airport Highlights the Need for Additional TSA Situational Awareness Management and Oversight Capabilities

The following events are described as they unfolded at MCO and SJU airports. Although SJU follows Atlantic Standard Time, all times indicated are Eastern Standard Time. On March 5, 2007, Delta Airlines Flight #933 was scheduled to depart from MCO at 11:00 a.m., and arrive in SJU at 1:41 p.m. Flight #933 was prepared to depart from the gate at 10:55 a.m., five minutes before its scheduled departure time.

Figure 2: Delta Flight #933 Schedule – March 5, 2007

Flight	From	To	Departure		Arrival	
			Scheduled	Actual	Scheduled	Actual
DL 933	MCO	SJU	11:00 a.m.	11:04 a.m.	1:41 p.m.	1:38 p.m.

Source: TSA, Delta Airlines, and www.flightstats.com

Just prior to Flight #933 leaving the gate, a police officer from the Orlando Police Department, Airport Division, received an anonymous tip that a specific airline employee was on board with a weapon. The police officer then placed a call directly to Delta Airlines at MCO, informing them of the situation. It remains unclear what information the Orlando Police officer specifically shared with Delta at this time, but in response to that call, the Delta Airlines duty manager at MCO ordered the aircraft held at the gate.

During the hold, officers from the Orlando Police Department removed Comair employee Zabdiel J. Santiago Balaguer (Balaguer) and his carry-on luggage from the flight. The Delta Airlines duty manager at MCO said he then talked to the captain of Flight #933, who said he was comfortable with departing from MCO. According to Delta Airlines, Flight #933 then taxied to the runway and departed at 11:04 a.m.

TSA's Initial Awareness of the Incident

According to TSA records, the Orlando Police Department placed a call directly to TSA personnel at MCO's East Checkpoint at 11:05 a.m. This appears to be the first communication TSA received regarding the situation with Flight #933. TSA's records indicate that during this call, a police officer informed TSA officials that a Delta flight was being directed to return to gate #73 due to a possible weapon on board. The Supervisory Transportation Security Officer who received the call from the Orlando Police Department notified a TSA Security Manager on-site, who in-turn notified TSA's local airport operations center. According to TSA records, incident notifications were sent to local TSA leadership at 11:07 a.m. Meanwhile, another TSA Security Manager and a Transportation Security Officer were dispatched to meet the aircraft at gate #73. Both individuals reported that upon arriving at the gate, the aircraft had departed, and police were already interviewing Balaguer.

TSA personnel then conducted a complete screening of Balaguer and his carry-on luggage. The only prohibited item they discovered during this search was a cigarette lighter. Balaguer was detained by the Orlando Police Department until the Federal Bureau of Investigation arrived to question him.

TSA records indicate that following the incident notifications, the Federal Security Director's senior staff at MCO made two bridge calls, at 11:17 a.m. and 11:26 a.m., respectively. A bridge call is a telephone conference call used by TSA field personnel to communicate with headquarters and other security partners in the event of a security incident. Each call ended after a few minutes.

TSA records indicate that the Greater Orlando Aviation Authority sent its own incident notification at 11:11 a.m. According to the Federal Security Director at MCO, after the plane's departure, the Greater Orlando Aviation Authority notified TSA that they suspected another airline employee could also be involved, based on a review of the access control systems. The access control logs, along with the closed-circuit television system, are used by the airport authority to monitor employees entering and leaving secure areas of the MCO airport.

Between 11:40 a.m. and 12:00 p.m., the Greater Orlando Aviation Authority confirmed with TSA at MCO that Thomas Anthony Munoz (Munoz) was likely on board Flight #933 with a large, black duffel bag that was never screened by TSA. Also, at this time, TSA and the Greater Orlando Aviation Authority did not know whether others were involved. Information from the flight manifest disclosed there were approximately 20 non-revenue passengers aboard the flight, including Balaguer and Munoz. The non-revenue passengers were employed by the airline and did not have to pay for the flight.

TSA Communications Between the Orlando and San Juan Airports While the Flight Was En Route

At approximately 11:30 a.m., the Federal Security Director from SJU received a call from the Federal Security Director at MCO advising him of a possible security breach concerning Flight #933 to

SJU. During this initial conversation, TSA records indicate that TSA officials from MCO and SJU decided to conduct a reverse screening of Flight #933 upon its arrival at SJU. A reverse screening is a search of all aircraft passengers and their luggage upon arrival as a result of intelligence or law enforcement-related information. TSA officials made the decision to reverse screen Flight #933 prior to the Greater Orlando Aviation Authority informing TSA officials at MCO about suspicions concerning the involvement of Munoz. From 12:17 p.m. to 1:00 p.m., TSA officials at SJU made arrangements to rescreen all people on board Flight #933 and their carry-on and checked luggage. Incident management of the possible security breach was handled directly between the Federal Security Directors at MCO and SJU.

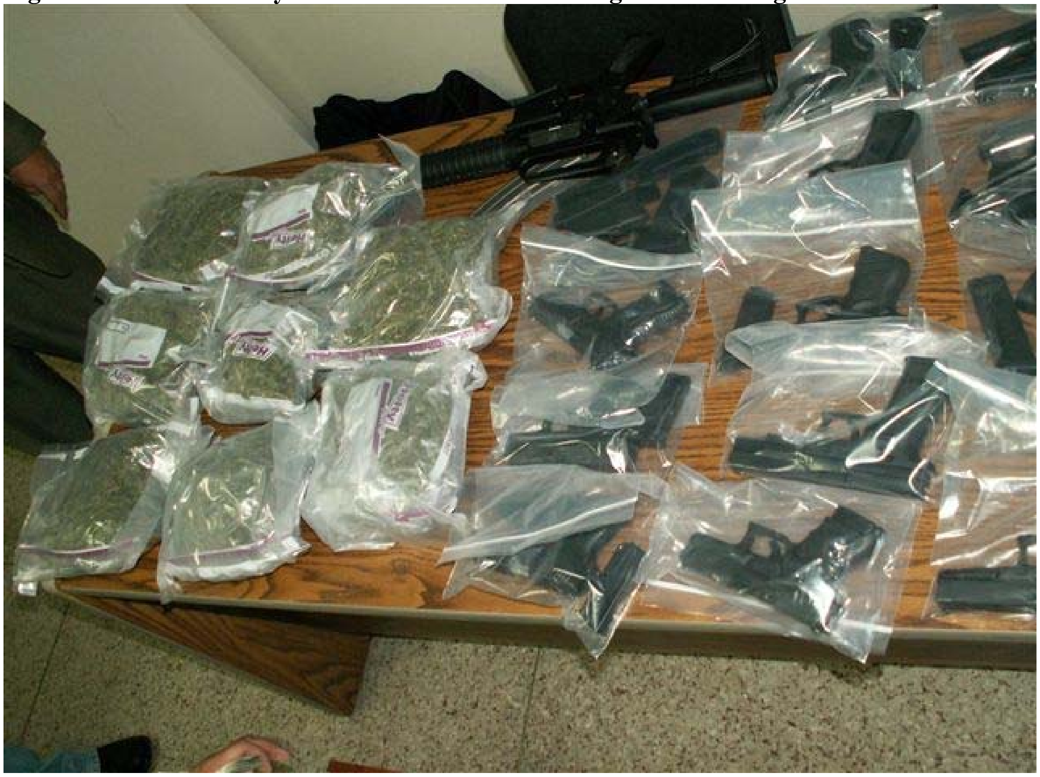
Reverse Screening in San Juan Identifies Munoz

At approximately 1:38 p.m., Delta Flight #933 arrived at SJU. After the flight landed and was taxiing to the terminal gate, a member of the Delta flight crew made an announcement over the aircraft intercom system that TSA was going to conduct a random screening of passengers exiting the aircraft. This announcement described the screening as a routine security measure.

According to TSA personnel at SJU, Munoz was one of the first individuals to exit the plane. He made a telephone call from his cellular phone while exiting the jet bridge. A TSA official present at the time said Munoz then approached the Transportation Security Officers conducting the screening. Munoz surrendered the black duffel bag in his possession, saying, “I’m busted.” After TSA personnel opened the bag, it was determined that Munoz was in possession of weapons. He was immediately taken into custody by the Puerto Rico Police Department.

A full inventory of the bag later revealed it contained 13 handguns, 1 M-4 assault rifle, and 8 pounds of marijuana, as shown in Figure 3. Munoz was subsequently turned over to the Bureau of Alcohol, Tobacco, Firearms, and Explosives for processing. TSA continued to screen every passenger and their luggage until the entire flight was cleared.

Figure 3: Full Inventory of Munoz's Black Duffel Bag on Board Flight #933



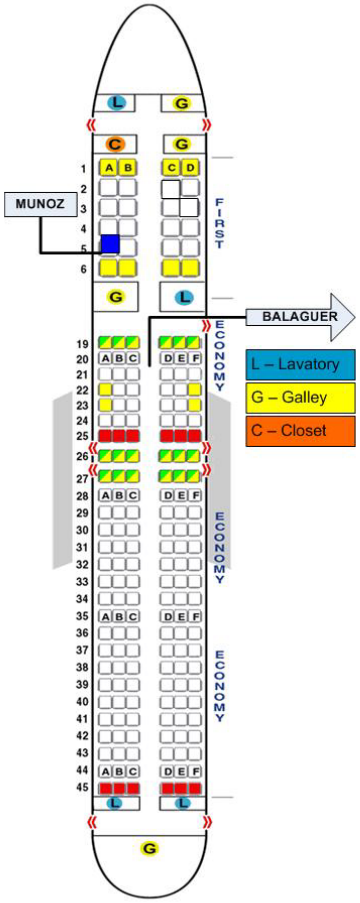
Details of the Incident Demonstrate Exactly How Orlando Airport Security Was Breached

During the Bureau of Alcohol, Tobacco, Firearms, and Explosives' initial interrogation of Munoz, he said that he was recently in a difficult financial situation. Shortly thereafter he was approached by fellow Comair employee, Balaguer, who offered him approximately $4,000 to $5,000 to accompany him on a trip to Puerto Rico to deliver firearms and marijuana. Munoz said that on the morning of March 5, 2007, he and Balaguer arrived at MCO around 3:00 a.m., wearing their work uniforms. Internal records from the Greater Orlando Aviation Authority verify that on March 5, 2007, at 3:39 a.m. Balaguer entered the secure area of the airport used to sort and load luggage.

At 3:44 a.m., closed-circuit television records show Munoz carrying a large black duffel bag inside the secure area. At 3:46 a.m. Balaguer exited the area; Munoz followed at 3:48 a.m. Closed-circuit television records again show Munoz exiting the secure area, this time without the black duffel bag. Munoz would later admit that he hid the duffel bag in the secure area during this timeframe. Munoz stayed at the airport while Balaguer left the airport.

Later that morning, Balaguer returned to MCO and processed through a TSA screening checkpoint as a flying passenger. Once at the departure gate, Munoz retrieved the black duffel. TSA records indicate that Munoz then hid in a bathroom for several hours with the duffel bag to avoid detection. Shortly before departure, Balaguer and Munoz boarded the aircraft separately. Munoz was seated in the first class cabin, while Balaguer was seated in the coach section of the aircraft and removed as shown in Figure 4.

Figure 4: Flight #933



Source: seatguru.com

After initially being released for lack of evidence, Balaguer was arrested at his home the following evening, March 6, 2007, by Special Agents from the Federal Bureau of Investigation, in conjunction with several other law enforcement agencies. In June 2007, Balaguer pleaded guilty to carrying a firearm during, and in relation to, a drug trafficking offense. In October 2007, he was sentenced to 15 years in federal prison. In February 2008, Munoz pleaded guilty and was sentenced to 30 months in federal prison.

Changes Made to Orlando Airport Security Operations As a Result of This Incident

Following the March 5, 2007, incident, the Greater Orlando Aviation Authority mandated that all employees with planeside access undergo screening. However, the Greater Orlando Aviation Authority officials said that despite being labeled 100% employee screening, these new security measures only cover employees with direct access to an aircraft. All employees entering the sterile or secure areas from the first level of the airport were already being screened through the passenger checkpoint.

At MCO, in addition to the first level screening, employee screening was instituted at employee-only checkpoints and at vehicle checkpoints on the airport perimeter. Before the incident, there were eight employee-only access points on the second level with no employee screening in place. These employee-only checkpoints provide employees who work outside the terminals with access to the secure area of MCO. Screenings at the access points are performed by TSA Transportation Security Officers.

All employees working inside the sterile area of the terminal beyond the passenger screening checkpoints are required to go through TSA passenger security screening on the third level of the airport. In addition to TSA's screening of airport employees, the Greater Orlando Aviation Authority performs vehicle and employee screenings at all three vehicle access points that lead to the secure area of the airport. Screenings at the vehicle access points are performed by a contract company. One contract employee verifies an employee's SIDA badge while others search the vehicles. Aside from the initial capital costs, estimated at $5.6 million, the Greater Orlando Aviation Authority said that its annual costs for sustaining their employee screening model could range from $1 million to $3 million.

TSA Needs To Improve Its Initial Situational Awareness Protocols

Although TSA's Security Directive 1542-04-11B requires that an airport operator immediately report to the TSA Federal Security Director all incidents and suspicious activities that could affect the security of U.S. civil aviation; in this case, the report was not immediate.[8] As noted earlier, TSA officials at MCO became aware of the incident after Flight #933 was en route to SJU. We determined that after the aircraft's departure, problems existed with the timeliness, accuracy, and efficiency of how information was processed and shared among airport security partners.

After the anonymous tip came into the Orlando Police Department, Delta Airlines was contacted first. When the police made this call, Flight #933 was preparing to depart from MCO. This contact from the Orlando Police Department was the only reason Flight #933 did not immediately take off with both Balaguer and Munoz on board.

Nevertheless, once TSA officials at MCO became aware that weapons might be on board Flight #933 and that an additional passenger might be involved, problems existed with communicating accurate and timely situational awareness of the incident.

[8] Aviation Security Directive, SD 1542-04-11B, Incidents and Suspicious Activities Reporting, December 8, 2004.

TSA's Situational Awareness of the March 5, 2007, Incident Was Not Adequate

Initially, problems began when the Federal Security Director at MCO and the Freedom Center, formerly known as the Transportation Security Operations Center, were not notified of the incident in a timely manner. The Freedom Center is the single point of contact for security-related operations, incidents, or crises within all U.S. land and air modes of transportation. The center is to obtain and maintain situational awareness of an incident, while allowing Federal Security Directors to manage an incident. The first notification that the center received came from Delta Corporate Security after the flight departed. Furthermore, the information provided to the Freedom Center at this time was inaccurate. Despite the fact that the aircraft departed at 11:04 a.m., TSA records indicate that Delta Corporate Security told the Freedom Center that Flight #933 was returning to the gate due to a report of a passenger on board with a weapon.

As noted earlier, by approximately 11:30 a.m., local TSA officials from MCO and SJU had decided to rescreen the flight upon its arrival in SJU. Between 11:40 a.m. and 12:00 p.m., the Greater Orlando Aviation Authority and TSA officials at MCO confirmed that Munoz was aboard Flight #933, and was probably in possession of a large, black duffel bag containing either weapons, drugs, or both. By all accounts, every interested party should have been aware that the flight was going to be rescreened by approximately 11:30 a.m., and aware that another suspect was on board by 12:00 p.m. However, TSA records indicate that inaccurate or untimely information continued to circulate among several key TSA officials until after 1:00 p.m. Figure 5 is an accounting of the erroneous or untimely exchanges that continued to circulate through TSA after 11:30 a.m.

Figure 5: Information Shared Within TSA

Telephonic Communications		Information
To	From	
Freedom Center	Federal Air Marshals' Mission Operations Center	Delta Flight #933 has been pulled back to the gate [at MCO] per law enforcement.
Freedom Center	TSA MCO	Employee from Delta Flight #933 deplaned for drugs.
Freedom Center	Delta Corporate Security	Delta Corporate was advised [by TSA] that Flight [#933] was arriving with 20 employees onboard with weapons and drugs; inquiring if aircraft needs reverse screening.
Federal Air Marshals' Mission Operations Center	Federal Air Marshals' Orlando Field Office	After calling in for a status update, the Orlando Field Office is informed that a passenger had bypassed security at MCO, but there was no weapon involved, per the Freedom Center. The Orlando Field Office contacts the Freedom Center for clarification
SJU	Freedom Center	SJU reports the flight will be rescreened upon arrival because it is believed another passenger might have weapons on board
Freedom Center	Federal Air Marshals [Location unknown]	Request made that the plane be reversed screened in SJU

Despite many serious concerns voiced about this security breach, TSA did not take corrective action in several areas.

- First, TSA made limited efforts to investigate the actions of Delta Airlines during this incident. We have concerns that Delta might have failed to meet its reporting responsibilities regarding the Aircraft Operator Standard Security Program. As the regulating entity, TSA should have conducted a full assessment of Delta Airlines' role to determine whether corrective action was necessary.

- Second, TSA never conducted any internal assessments to determine why inaccurate or untimely information continued to circulate throughout the organization after 11:30 a.m.

- Finally, the information concerning this breach disseminated throughout TSA, in its Tuesday, March 6, 2007, Executive Daily Summary, inaccurately included information that "parts of weapons and drugs were found and seized." It also omitted any mention that the two individuals involved were airline employees.

TSA could have capitalized on a unique opportunity to assess its situational awareness capabilities, and redefine its response protocols and criteria to mitigate similar, future security breaches.

At the time of the incident, TSA policies did not cause MCO to be susceptible to the security breach, nor did TSA have an opportunity to respond prior to the aircraft's departure from MCO. However, TSA's inability to obtain and maintain adequate situational awareness, and continued circulation of inaccurate and untimely information, raise concerns regarding TSA's oversight responsibilities.

Recommendations

We recommend that the Assistant Secretary for the Transportation Security Administration:

Recommendation #1: Enact national security measures that ensure TSA has the opportunity to clear an aircraft for departure when law enforcement officers intervene prior to a scheduled departure.

Recommendation #2: Evaluate the March 5, 2007, incident at the Orlando International Airport in Florida, develop an assessment of Delta Airlines' role, and determine whether incident management protocols, oversight responsibilities, or training procedures need to be revised.

Management Comments and OIG Analysis

We evaluated TSA's written comments and have made changes to the report where we deemed appropriate. A summary of TSA's written response to the report's recommendations and our analysis of the response follows each recommendation. A copy of TSA's response, in its entirety, is included as Appendix B.

TSA Response: TSA concurred with Recommendation 1. In its response, TSA management said they have adopted national security measures to ensure that TSA has the opportunity to clear an aircraft for departure when law enforcement officers intervene prior to a scheduled departure. These measures are outlined in a TSA/Federal Aviation Administration joint operating procedures memorandum and a TSA-issued security directive to airport operators.

In October 2004, TSA and the Federal Aviation Administration developed joint operating procedures to provide Air Traffic Managers and Federal Security Directors with guidance for responding to both immediate and non-life threatening situations. The guidance states in part that, "if in the opinion of the Federal Security Director, there is an imminent and potentially life threatening security situation, the Air Traffic Managers, consistent with safety, will comply with the Federal Security Director's requested operational response.

Additionally, TSA issued a Security Directive (SD 1542-04-11B) on December 8, 2004, which requires airport operators to immediately notify Federal Security Directors of all incidents and suspicious activities that could affect the security of U.S. civil aviation. The Aircraft Operator Standard Security Program also requires aircraft operators to notify the Freedom Center immediately of suspicious activities that could affect the security of aviation. TSA is considering procedural changes to ensure that Federal Security Directors also receive timely notification of such reports.

OIG Analysis: We consider TSA's proposed actions responsive to the recommendation, which is resolved and open. This recommendation will remain open until procedures are in place to ensure that TSA is notified when law enforcement intervenes with a flight prior to departure. TSA should also consider that resources are made available to respond timely to affected flights, in an effort to limit potential flight delays.

TSA Response: TSA concurred with Recommendation 2. In its response, TSA management said after the March 5, 2007, incident, TSA and the stakeholders at the Orlando International Airport held a series of meetings and made several improvements, including meeting with the Delta Station and Operations Managers on duty during the incident and changing the reporting procedures to ensure TSA is immediately notified whenever law enforcement is called to an aircraft. TSA will review the actions taken at MCO, develop best practices to share with all Federal Security Directors and encourage implementation at other airports.

OIG Analysis: We consider TSA's proposed actions responsive to the recommendation, which is resolved and open. This recommendation will remain open pending the receipt of documentation that demonstrates:

- Orlando TSA and the Greater Orlando Aviation Authority changed the reporting procedure to ensure TSA is immediately notified whenever law enforcement is called to an aircraft;
- Orlando TSA changed the process to ensure TSA senior staff is notified of all law enforcement calls to aircraft;
- Orlando TSA, the Greater Orlando Aviation Authority, and other stakeholders including law enforcement conducted tabletop exercises to test incident management protocols; and,
- Greater Orlando Aviation Authority Airport Security Plan change that delineates and clarifies the reporting requirements from the airport to TSA.

TSA Needs Changes to Improve Security and Its Regulatory Oversight of Non-TSA Airport Employees

Since the March 5, 2007, incident, TSA has taken steps in several areas to improve its overall security posture at airports, including the introduction of its Security Threat Assessment vetting, as well as mandating that all airports implement an ADASP program.

Regulatory Framework is Outdated

While these changes have improved overall airport security, additional changes are necessary to enhance the security posture of airports nationwide. Specifically, TSA conducts oversight of non-TSA employees' at all federalized airports. TSA's oversight covers a number of different areas, including an airport's security program, and its badging process and challenge program. However, the regulatory framework that TSA relies upon to conduct its oversight is outdated, and does not adequately address the vulnerabilities associated with the insider threat stemming from any employee with knowledge about an airport's internal operations.

For example, during our fieldwork, we determined a number of airports, on their own initiative, have significantly improved security by implementing practices and measures that exceed the basic requirements of the airport security program.

Specifically, the program requires all airports have an access control system to prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into and within the secured area. While some airports we visited have a three-tier biometric access control system in place, others rely on a basic one-part swipe of a SIDA badge as their access control system.[9] Although employees are required to immediately report a lost badge, one-part swipe systems could enable anyone to gain access to a secure area by simply obtaining a badge from an airport employee. While the one-part swipe system is acceptable under the current regulations, it provides no assurance that the person using the badge is the same person who was cleared through the criminal history records check and Security Threat Assessment vetting processes. Through the use of the one-part swipe system, anyone who obtains an active SIDA badge could potentially circumvent an airport's security by gaining access to the secure areas of an airport.

Furthermore, while the name-based Security Threat Assessment is conducted on a recurring basis, conducting the criminal history records checks is only required when an employee is initially hired. As long as an employee maintains continuous employment, a subsequent criminal history records check is not performed. When an employee is convicted of a disqualifying criminal offense during employment, the employee is required to report the offense to the airport operator and surrender his or her access medium within 24 hours of the conviction or a finding of not guilty by reason of insanity.[10] However, we were told by a number of airline and airport officials that employees will not voluntarily disclose this information because the employees know they will lose their jobs.

[9] A three-tier biometric access control system requires confirmation of a valid SIDA badge, input of a personal identification number, and identity confirmation through biometrics before access to the secure area is permitted.

[10] 49 CFR § 1542.209 (l)(2).

Also, TSA regulations do not have a requirement to conduct financial checks on airport employees. In regard to the March 5, 2007, incident, one of the individuals arrested said his financial problems led to his involvement in smuggling guns and drugs from Orlando to San Juan.

One airport authority Director of Security said changes are needed to help harden the vulnerabilities associated with the insider threat. This includes implementing new regulations that govern the behavior of airport employees, particularly a requirement for all airport employees to have recurrent criminal history record checks. The Director of Security said TSA needs to modify its official guidance and regulations, instead of issuing repeated TSA Security Directives, which imply "temporary" changes. The Director also said airport authorities are reluctant to make substantial changes based upon Security Directives, because directives are subject to change on short notice.

Additional Changes Can Enhance the ADASP Program

The ADASP program is designed to facilitate random and unpredictable screening of airport employees and vehicles entering any location or route that provides access to secure, sterile, and air operation areas. Although the program was established recently, most airport authorities, airlines, airport police, and vendors we interviewed said ADASP is an effective deterrent against airport employees bringing prohibited items to the airport. However, airport employees know the ADASP program is based on random screenings, so some might wait until the ADASP team leaves a particular location, or they might use another entry point. We were also told that employees use their cell phones to alert other employees about ADASP locations to avoid screenings.

During fieldwork, we noticed inconsistent implementation of ADASP screening at employee entrance doors. At most airports, we observed the ADASP teams setting up screening stations in front of the employee access doors to the secured area. At several airports we observed employees turning away after seeing the ADASP screening station. At another airport, the screening station was set up inside the employee entrance door. By placing the ADASP team inside, employees were unaware of the screening until opening the door to enter the secured area. Once the door was open, it was too late for employees to use another access door.

Also at one airport, we observed close coordination between the law enforcement officers and the ADASP team. Both shared schedules and law enforcement officers accompanied the ADASP team while conducting vehicle gate screenings.

Furthermore, TSA should consider requesting access control logs from airport authorities to conduct usage analyses. By analyzing the logs, they can determine whether airport employees are using other entrances when the ADASP teams are stationed at access points.

TSA Plans Several Changes to Improve Security and Its Regulatory Oversight

Officials from TSA's Office of Security Operations said that TSA wants to move forward with the rulemaking process to require airports to conduct stricter employee background investigations. Also, TSA wants to improve the monitoring of unattended access points, such as perimeter fences, and mandate the upgrade of all access control systems to meet certain biometric specifications. TSA envisions these improvements taking four to five years to implement. Office of Security Operations officials said the initial comment period for these regulatory changes should begin before the end of calendar year 2008. We are encouraged that the proposed changes, once implemented, would improve security and enhance TSA's regulatory oversight of airports nationwide.

In addition, TSA has partnered with several industry and private sector groups, including Airports Council International and the American Association of Airport Executives, and has identified six alternatives to 100% employee screening that would help mitigate the insider threat at airports. These alternatives include:

- Enhancing behavioral recognition training for segments of airport employees;
- Increasing random inspections;
- Enhancing training for all airport employees;
- Developing biometric access controls;
- Improving employee background screening; and,
- Deploying additional technologies.

TSA's Administrator Hawley has advocated against committing TSA "to inflexible, resource-intensive measures" that are not consistent with its risk-based approach to aviation security.[11] While TSA has taken preliminary steps to address the insider threat some employees might present at airports, additional work is necessary to ensure that an employee accessing the sterile and secure areas of an airport is the actual person vetted and approved to work in those areas.

Recommendations

We recommend that the Assistant Secretary for the Transportation Security Administration:

Recommendation #3: Change the regulatory requirements to include provisions for mandating phased-in biometric access controls for airport operators, and recurrent criminal history and financial records checks for Secure Identification Display Area badge employees.

Recommendation #4: Apply effective and consistent Aviation Direct Access Screening Program policies and procedures at all airports.

Recommendation #5: Establish an Aviation Direct Access Screening Program working group to consider policy and procedure changes based on an accumulation of best practices across the country.

Management Comments and OIG Analysis

TSA Response: TSA concurred with Recommendation 3. In its response, TSA management said it has initiated the process to include provisions for a phased-in biometric access control system for airport operators. TSA is working on standards for biometric access controls systems and recurrent criminal history records checks for employees with unescorted access to SIDA portions of airports. As for financial records checks, TSA officials said they will take the recommendation into consideration.

[11] Testimony of Administrator Hawley before the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection. April 19, 2007.

In addition, several recently issued documents provide a broad perspective of TSA's current thinking about biometric smart cards and their application at airport access control points. In May 2008, TSA released the *Aviation Credential Interoperability Solution Technical Specifications* to airport and aircraft operators for review and comment. This document discusses many of the technical issues that TSA will consider in establishing standards. Also, an advisory committee sponsored by the Federal Aviation Administration recently issued a document that may encourage the use of biometrics at airports, RTCA DO *230-B Integrated Security System Standard for Airport Access Control, June 19, 2008*. The document aggregates industry best practices for employing perimeter security measures, including the use of biometric smart cards at access control points. TSA will consider the document when developing its standards.

Furthermore, TSA management said they completed the employee screening pilots at seven airports as mandated in the *Consolidated Appropriations Act of 2008*. TSA and the Homeland Security Institute, an independent contractor, will evaluate the result of the pilots and report back to Congress as mandated in the Act.

OIG Analysis: We consider TSA's proposed actions responsive to the recommendation, which is resolved and open. The recommendation will remain open pending receipt of TSA's finalized standards for the phased-in biometric access controls for airport operators and the pilot program results.

TSA Response: TSA concurred with Recommendation 4. In its response, TSA management said to facilitate consistency in applying ADASP procedures, TSA established an ADASP Coordination Team in April 2007. Part of the team's responsibility is to respond to ADASP questions from the field. The questions and responses are made available to all Transportation Security Officers. The Coordination Team also reviews the ADSAP standard operating procedures to determine whether revisions are necessary to clarify procedures.

OIG Analysis: We consider TSA's proposed actions responsive to the recommendation, which is resolved and closed. No further reporting is necessary.

TSA Response: TSA concurred with Recommendation 5. In its response, TSA management said they formed a headquarters ADASP Coordination Team in April 2007. This team consists of personnel from TSA's Procedures Division (part of the Office of Security Operations), Special Screening Programs, Transportation Security Network Management, Office of Chief Counsel, and Office of Compliance. The team collaborates when changes to the ADSAP procedures are suggested, including at the conclusion of an ADASP Pilot or special operation, and when questions regarding ADASP procedures are received from the field. The headquarters ADASP Coordination Team reviews the questions and provides clarification and guidance by posting the response on an electronic database accessible to all Transportation Security Officers.

OIG Analysis: We consider TSA's proposed actions responsive to the recommendation, which is resolved and closed. No further reporting is necessary.

100 Percent Airport Employee Screenings Raises Feasibility Issues

The March 5, 2007, incident at MCO, and subsequent media coverage renewed longstanding concerns about airports and the vulnerabilities associated with the insider threat. Even with improvements to its current oversight of non-TSA airport employees, some airport industry partners, private sector groups, and Congress are calling for 100% airport employee screening. While there is no current agreed upon definition of what 100% airport employee screening is, there are a number of important questions that need to be answered:

- What is the purpose of 100% screening   to prohibit threat objects from entering the secure areas of an airport or to focus more broadly on smuggling or other criminal activities?

- Who will screen airport employees   TSA or contracted personnel?

- Will employees be screened to the same standards required of passengers? And if so,

- How will exceptions be made for prohibited items   from box-cutters to blowtorches   which are required by certain employees to perform their jobs?

The answers to these questions will affect the structure and costs associated with any model of 100% airport employee screening. Industry experts estimate that implementing a generalized version of employee screening, across the entire federalized aviation system, could cost anywhere from $3 billion to $6.5 billion annually.[12]

The vast majority of people are only familiar with airports from the passenger's perspective. Their frame of reference is limited to those processes that directly affect them from check-in and passenger screening, through the boarding process. However, there is additional activity at the airport that the average passenger does not see; activity that is vital to the operational health of an airport. This activity includes vendor and cargo deliveries, airplane maintenance and fueling, airport construction, and grounds keeping, among others. During our fieldwork, we visited seven airports to assess the challenges associated with screening employees performing functions tied to these processes. We met with more than 120 local representatives from TSA, airport authorities, law enforcement, and various business interests.

Perspectives from TSA's Field Workforce

Overall, TSA's senior management in the field, assuming they would be charged with implementing any measures associated with 100% airport employee screening, expressed concern about implementing such a mandate.

One Federal Security Director believed it was important to have the capability to perform increased, or even 100% airport employee screenings in response to some specific intelligence, but remained skeptical that permanent employee screening was necessary. Another Director believed it would be unwise to consider making any changes to TSA's current security posture unless a 100% employee screening solution was targeted.

Regardless of one's position on this issue, all TSA personnel that we encountered seemed to agree that any additional responsibilities would require a substantial influx in personnel and additional resources. One Assistant Federal Security Director for Screening said that it would necessitate a "parallel" workforce to screen all airport employees. For FY 2008, TSA's screener workforce totals 45,438 full time personnel, including 1,100 managers, with a budget of approximately $2.64 billion. Thus, creating a parallel workforce would necessitate an additional 45,000 employees and approximately $2 billion annually to screen all airport employees.

[12] United States Commercial Aviation Partnership (USCAP). *Report on USCAP Analysis of H.R. 1413 and Alternatives*. October 2007.

Another Federal Security Director pointed out that the toughest change would be ensuring every airport had the local buy-in of the airport community. For example, mandated employee screenings would require additional support from local law enforcement, which may or may not be currently feasible at certain airports.

Concerns Raised by Airport Authorities and Local Law Enforcement

At each of the airports visited, we spoke with local airport authorities and law enforcement about the issue of 100% employee screening. Of the seven airports we visited, three had specific experiences with employee screening.

At one airport, TSA assisted with a pilot screening program that focused on screening a select portion of airport employees with access to passenger aircraft. The pilot screening program was conducted for six weeks, and it was limited to only one of the airport's terminals. During our discussions with officials, we were informed that 100% employee screening was feasible at this airport, but cautioned that consideration would have to be given to providing airports with the appropriate number of Transportation Security Officers to perform this additional tasking. Officials also raised several practical concerns that would have to be addressed should permanent employee screening be implemented at every terminal, to include the construction of additional bathrooms on the sterile side and the relocation of a trash compacting facility in the public area.

At another airport, officials from the airport authority and the airport's police department noted that after September 11, 2001, the airport immediately closed all its employee access portals and required everyone to go through a passenger screening checkpoint. The airport authority eventually reverted to allowing employees to go through a reduced number of employee access points, given the negative effect the additional employee volume was having on passenger screening. However, the reopening of the employee access points was accompanied by enhancements to the airport's access control system, which currently includes a biometric hand-reader system. One airport official said that individuals began to question the screening of employees, given that many already had what they needed in the sterile area to "take down" an aircraft. Finally, the airport authority said employee screening requirements would necessitate around-the-clock staffing, particularly at large airports, to meet their operational needs.

In addition, another airport authority has employed a third-party contractor since 1999 to deter theft, as well as verify the identity and validity of all employees using their SIDA badges to access the secure area. While not solely focused on screening employees before they enter the secure area, the contractor does play an important role toward enhancing the overall security posture of the airport.

Opinions at the other airports we visited varied. However, one concern all airport authorities raised was the likelihood that any development would require significant infrastructure modifications to meet new operational requirements.

Concerns Raised by Airport Business Partners

At each airport visited, we met with various commercial interests, including airlines, concessionaires, vendors, and union officials to discuss this issue. These stakeholders raised many of the same concerns, which could be grouped into three inter-related categories: operations, resources, and costs.

With regards to the effect employee screening would have on airport operations, a number of entities expressed concern regarding how employee screening might negatively affect their productivity. Many businesses rely on efficient shift changes and dual-use employees who repeatedly transition between the public and secure areas of an airport. One hundred percent employee screening would mean that the same employee would have to be rescreened after each egress into the public area before returning to the secure area.

Tied to these operational concerns is the question of how these new procedures would be implemented. Currently, most airport employees use the nearest access point to enter the secure area in the normal course of their duties. However, it is widely assumed that should employee screening be mandated, most airports would have to close a number of access points to funnel employees into specific areas to reduce the costs associated with employee screening. This would force those areas to continually process large numbers of employees on a regular basis. Assuming TSA would be responsible for employee screening, this scenario would require those areas to be adequately staffed, in some cases on a 24-hour basis, to handle the volume of traffic. Many airport business partners are concerned that TSA would not be adequately staffed to deal with this new mandate, which would cause processing delays.

Finally, should TSA or a contract entity be adequately staffed, almost all airport business partners are concerned about how this added requirement would be funded. The two options discussed target either:

- TSA, which would necessitate a substantial increase in its annual budget, or
- The airport operators or airlines, which would likely pass those additional costs to passengers through increased ticket prices and processing fees.

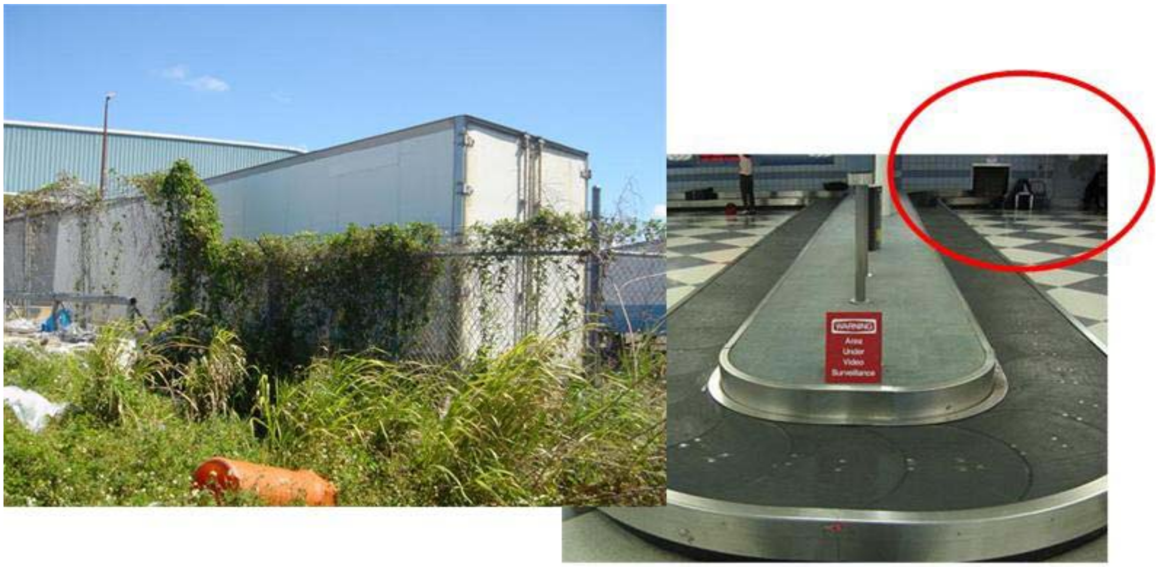
Vulnerabilities Would Persist With 100 Percent Airport Employee Screenings

Should 100% airport employee screening be implemented, certain vulnerabilities would persist. Mitigating some of those vulnerabilities requires the introduction of technological solutions, infrastructure upgrades, or some combination of each; even then, no assurances can be made. Please see Appendix E for a four-page depiction of a typical airport layout.

Employees and Contraband Baggage

When discussing persistent vulnerabilities, several TSA officials said that two relatively easy ways to introduce contraband into the secure area would be for someone to throw a bag over a perimeter fence or pass a piece of luggage through a baggage claim to an awaiting accomplice. At some airports, baggage belts revolve between the public and secure areas of an airport's baggage make-up area, which is an airport's baggage staging area used to load and unload airline baggage.

Figure 6: Airport Perimeter Fence Line at a Category X Airport and Baggage Claim Egress from Public Area to Secure Area



Source: www.upgradetravelbetter.com

While such methods are extremely basic and relatively crude, numerous TSA and local airport officials expressed concern regarding these two possibilities. One TSA official said he personally witnessed an attempt to throw a bag over a perimeter fence at a particular airport we visited. These vulnerabilities could be mitigated with improvements to the perimeter controls and baggage claim systems at airports. However, depending on the size of the facility and the current state of perimeter controls or baggage claim systems, these upgrades could be costly at most airports.

Airline Catering and Provisioning and Vendor Deliveries

Another method for exploiting commercial aviation involves the airline catering and provisioning or vendor deliveries that occur daily at airports across the country. Airline caterers and provisioners supply aircrafts with meal service for domestic and international flights, while vendors, as defined by TSA, include anyone who is authorized to conduct business in the airport. Vendors supply all the food and consumer goods sold at the airport. Typically, the catering and provisioning deliveries are made through an airport vehicle access gate. Vendor deliveries can be made curbside at a terminal, at a vehicle access gate, or both, given the policies and layout of an airport. Depending on the size and volume of an airport, this can amount to hundreds of daily around-the-clock arrivals.

According to the Aircraft Operator Standard Security Program, an aircraft operator employee or authorized representative not employed by the catering company, is required to ensure that each catering vehicle is sterile before any catering carts can be loaded for delivery.[13] An inspection of catering carts must also be performed prior to the employee either securing the vehicle with a tamper-proof seal or escorting the vehicle directly to aircraft.

TSA security directives require the airport operator to inspect vendor personnel and deliveries at all sterile area access points, other than the screening checkpoint, to ensure the security of the merchandise.[14] Some Federal Security Directors have enacted stricter requirements for vendors. For instance, two airports have either developed or are pursuing centralized "commissary" or "dock" facilities to screen all shipments arriving to the airport; however, few other airports have or are contemplating a similar approach.

In addition, law enforcement agencies have recognized the vulnerabilities associated with these two processes for years. One of the largest known criminal enterprises within the aviation industry relied on both baggage handlers and catering employees to smuggle drugs on board commercial aircraft. In 1999, the U.S. Customs Service, now U.S. Customs and Border Protection; the Bureau of Alcohol, Tobacco, and Firearms, now the Bureau of Alcohol, Tobacco, Firearms, and Explosives; and the Drug Enforcement Agency obtained 58 indictments of individuals connected to this narcotics smuggling enterprise operating out of Miami International Airport in Florida.

Cargo Facilities

Finally, approximately 7,500 tons of commercial cargo are transported on passenger aircraft daily. We have identified vulnerabilities of the oversight of passenger aircraft cargo in the past.[15] However, after improvements are made, contraband can still be secretly brought into an airport's operation area. At many

[13] Security of vendor and catering deliveries are covered under the Aircraft Operator Standard Security Program, unless otherwise amended locally. See Aircraft Operator Standard Security Program, April 22, 2008.

[14] Transportation Security Administration Security Directive 1542-06-01D. The local Federal Security Director is permitted to approve alternative site specific procedures as needed.

[15] *Transportation Security Administration's Oversight of Passenger Aircraft Cargo Security Faces Significant Challenges* (Redacted). Department of Homeland Security Office of Inspector General. OIG-07-57, July 2007.

airports, large cargo facilities effectively function as the boundary between the public and sterile areas of an airport. This poses a unique challenge for those responsible for ensuring the security of these facilities because of the constant movement of goods to and from an aircraft.

While 100% airport employee screening is feasible, there are many unanswered questions as to how it would be implemented. These questions, raised by TSA, industry partners, and private sector groups alike, are valid and need to be addressed prior to taking any steps toward implementing 100% airport employee screening. Should these concerns not be addressed prior to implementation, TSA will be applying resources to a system that is prone to vulnerability.

Achieving an Integrated, DHS-Wide Perspective on Security at Airports Is Needed

The March 5, 2007, MCO incident highlighted the need for accurate and timely coordination and communication between all local security partners at an airport. Given the complexity of the airport environment, and the diverse, and sometimes overlapping responsibilities among key partner organizations, timely and effective communication can be achieved only when interagency relationships are already formally established and exercised prior to an operational crisis.

At some airports, local partner organizations have developed effective working relationships, often on an informal or ad-hoc basis. For example, at one airport, we learned that all the local partners regularly participate in TSA-led mock exercises, which help foster a sense of cooperation among those who would be called upon to act in the event of an emergency. These exercises, along with the airport's daily security meetings, provide partners with the opportunity to establish open lines of communication and build relationships where they did not always previously exist.[16] Unfortunately, as we learned through discussions with partner organizations at several other airports, strained relationships and a lack of formal procedures have affected the ability of many airport communities to deal with routine situations as well as potential emergencies.

While DHS officials at the airports would agree that better interagency coordination is a desirable goal, it is not easily achieved. As TSA officials

[16] The daily security meetings at this airport are attended by TSA, airline and concession managers, and other federal, state, and local governmental partners.

continue to pursue measures that encourage better communication and operational practices within airport communities, DHS should also use all of its component capabilities, together within the aviation environment, to ensure the DHS-wide mission is accomplished. At many airports across the country, other DHS components most notably U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement already perform their mandated roles and missions. However, efforts to assist another component with its mission are difficult, in part because these attempts are not tied to shared funding, resources, evaluations, or operational exercises. As a result, there are no current incentives to ensure cross-component cooperation, especially when it comes at the expense of trying to meet component-specific operational responsibilities.

Aside from the aforementioned VIPR Program, most airports have not established any DHS-wide cooperative efforts. At certain airports, TSA has been able to establish strong working relationships with other DHS counterparts, but this does not necessarily translate into ongoing cross-component cooperation. As a department, DHS must work toward institutionalizing cooperation across components in service of its overarching mission, similar to the efforts of the Department of Defense's Combatant Commands or the Federal Bureau of Investigation's Joint Terrorism Task Forces.

An organization that could be used as an applicable model for ensuring synergy across DHS mission-sets would be the Joint Interagency Task Force-South, a federal interagency task force that combines personnel from the military, law enforcement, and intelligence communities in an effort to combat illicit trafficking operations in the Southern Hemisphere. The integration of personnel from different agencies has been successful because the task force has a clear, comprehensive mission supported by a unified, joint command. Furthermore, the Joint Interagency Task Force-South command has identified collective metrics that can be divided into more narrowly defined pieces that closely mirror the core function of each parent organization. This allows the components to satisfy their parochial interests while serving a broader mission.

Conceptually, DHS could adapt a similar model to integrate its functional operation, given that several components already have a large presence at select airports. To be successful, an airport task force would require a unified command structure, shared resources, collective metrics, and an overarching mission. This model could be scaled to fit a regional configuration, which could be overseen by a senior regional director who would be responsible for all DHS-related activities in that region.

An airport with established intercomponent working relationships is more desirable to implement such a pilot program. While any collaborative model will take significant time to implement, refine, and institutionalize across DHS, it is important that the components begin focusing on the department's broader mission, rather than individual mandates, roles, and responsibilities.

Recommendations

We recommend that the Assistant Secretary for the Transportation Security Administration, in conjunction with the Director of Operations Coordination and Planning, and in coordination with other department and component principals:

Recommendation #6: Establish an intercomponent working group among U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and TSA, with the goal of piloting an integrated, DHS-wide operational concept at select airports.

Management Comments and OIG Analysis

TSA Response: TSA concurred with Recommendation 6. In its response, TSA management said that at airports with a combination of international and domestic operations, TSA already partners with U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, as well as the Federal Bureau of Investigation, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the U.S. Drug Enforcement Administration, and state, local, and airport police. TSA said these partnerships demonstrate an integrated DHS operational concept. TSA management said it will coordinate with its colleagues within DHS to discuss the feasibility of establishing a DHS-wide pilot at select airports that have ports of entry.

OIG Analysis: We consider TSA's proposed actions responsive to the recommendation, which is resolved and open. The recommendation will remain open pending the receipt of documentation that discussions on the feasibility of establishing a DHS-wide pilot program have taken place.

Conclusion

A few months after the arrests of Munoz and Balaguer, another MCO airport employee agreed to smuggle several firearms on board a commercial aircraft destined for Puerto Rico during a conversation with an undercover informant. According to published reports, the former JetBlue Airways baggage handler, Hiram Rivera-Ortiz, was taken into custody in August 2007. After his arrest, Rivera-Ortiz reportedly showed federal agents how easy it was to smuggle guns past airport security at MCO. Rivera-Ortiz is currently serving 70 months in federal prison.

This incident reinforces our initial concern about placing a high reliance on 100% airport employee screening to address existing airport vulnerabilities. Even with a configuration that is conducive to implementing 100% employee screening, the insider threat at MCO remains a concern. Furthermore, airports with more access points, multiple terminals, larger cargo operations, and fewer resources to allocate to upgrades have vulnerabilities that are that much more palpable.

The concept of 100% airport employee screening is feasible. However, we do not believe it is realistic at this time. Regardless of the amount of funding, resources, and effort allocated toward this endeavor, vulnerabilities will persist. While the intelligence, screening, and law enforcement communities continue to make progress in addressing these vulnerabilities, 100% airport employee screening cannot entirely bridge existing gaps. As TSA changes its regulatory requirements, technology improves, and airports upgrade existing security measures, implementing this concept would be more realistic and should be revisited.

We assessed a March 5, 2007, security breach where two Comair Airline employees at the Orlando International Airport successfully smuggled 14 firearms and 8 pounds of marijuana on board a Delta Airlines commercial airplane bound for San Juan, Puerto Rico. Our review was in response to requests from Representative Bennie G. Thompson, Chairman of the House Committee on Homeland Security, and Representative Ric Keller. The objectives of our review were to determine:

- whether TSA's actions and communication surrounding the March 5, 2007, incident were appropriate and effective;
- whether TSA's oversight of non-TSA airport employees is adequate; and
- the feasibility of 100% airport employee screening for individuals accessing an aircraft or the secure areas on an airport.

To accomplish our objectives, we interviewed or received documentation from TSA officials at MCO and SJU, the Greater Orlando Aviation Authority, Delta and Comair Airlines at MCO, TSA's Federal Air Marshal Service, and the Freedom Center. We also evaluated TSA's current and former processes for conducting airport employee screenings at MCO.

To assess the overall effectiveness of TSA's current airport employee screening practices and to determine the feasibility of mandating 100% airport employee screening, we conducted site visits at five other airports. During site visits, we reviewed current local airport employee screening practices, the background screening processes used for airport employees, and the SIDA badge monitoring and oversight of airport employee access controls.

At each airport, we met with relevant TSA personnel, including the Federal Security Directors, the Assistant Federal Security Directors, and Transportation Security Officers. We also met with a number of TSA's partner organizations, including each airport authority, several commercial airline representatives, airport concessionaires, aircraft catering companies, and union officials to discuss their views on the feasibility of 100% airport employee screening.

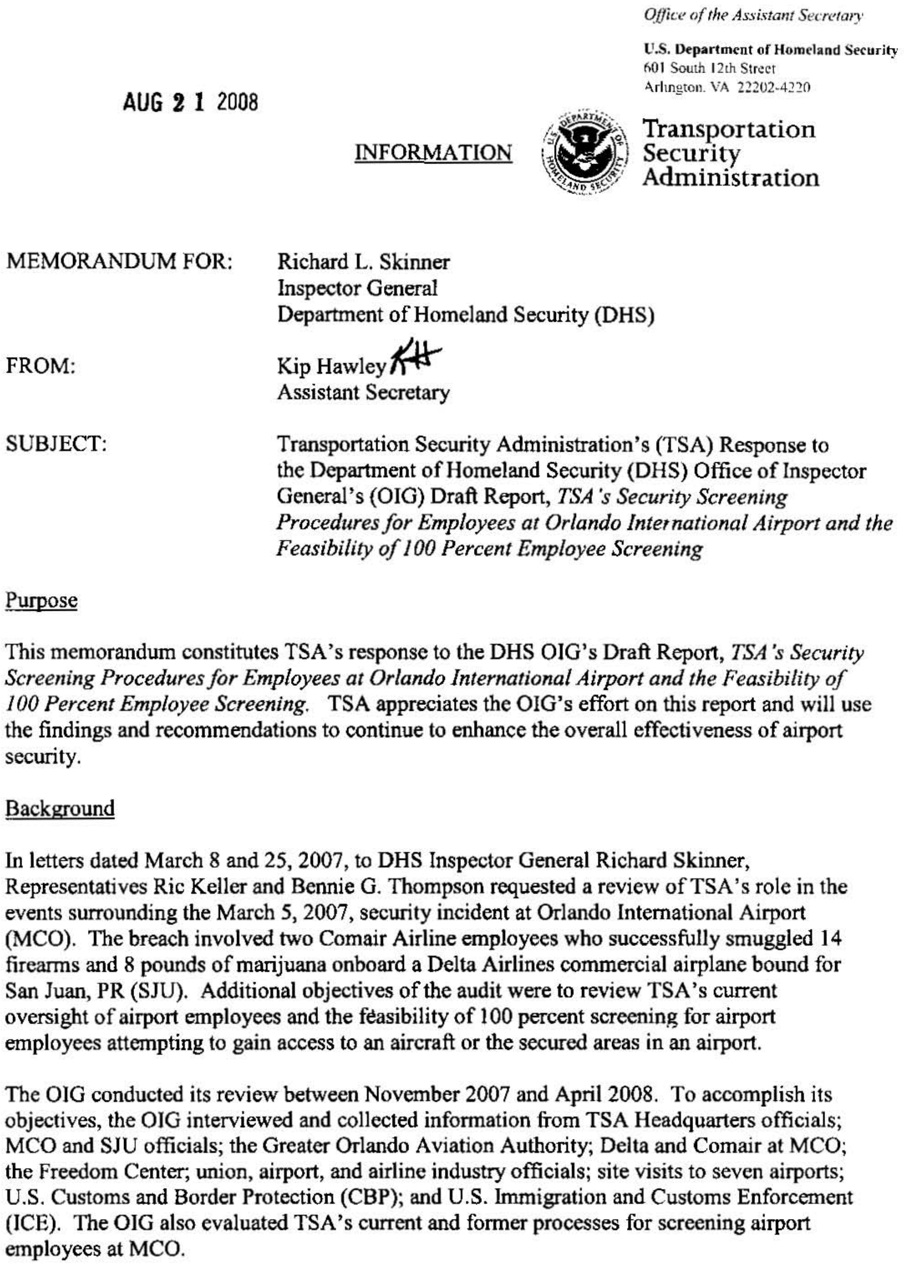
We also held meetings with union, airport, and airline industry officials including the American Federation of State, County and Municipal Employees; the American Federation of Labor and Congress of Industrial Organizations; the International Association of Machinists and Aerospace Workers; the Airports Council International; the American Association of Airport Executives; the International Air Transport Association; and the

Airline Pilots Association to obtain their views on the feasibility of 100% employee screening.

We interviewed more than 160 people including TSA personnel from TSA headquarters, the Office of Security Operations, the Office of Transportation Threat Assessment and Credentialing, the Office of Transportation Sector Network Management, Office of Law Enforcement, Office of Inspection, Federal Air Marshal Service, and the Freedom Center. We also spoke with personnel from U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement.

We reviewed relevant laws, regulations, policies, procedures, statistical information, and airport practices related to these three areas. Our fieldwork began in November 2007 and concluded in April 2008. We initiated this review under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections*, issued by the President's Council of Integrity and Efficiency.

Appendix B
Management Comments to the Draft Report



Office of the Assistant Secretary

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

AUG 2 1 2008

INFORMATION

Transportation
Security
Administration

MEMORANDUM FOR: Richard L. Skinner
Inspector General
Department of Homeland Security (DHS)

FROM: Kip Hawley KH
Assistant Secretary

SUBJECT: Transportation Security Administration's (TSA) Response to the Department of Homeland Security (DHS) Office of Inspector General's (OIG) Draft Report, *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening*

Purpose

This memorandum constitutes TSA's response to the DHS OIG's Draft Report, *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening.* TSA appreciates the OIG's effort on this report and will use the findings and recommendations to continue to enhance the overall effectiveness of airport security.

Background

In letters dated March 8 and 25, 2007, to DHS Inspector General Richard Skinner, Representatives Ric Keller and Bennie G. Thompson requested a review of TSA's role in the events surrounding the March 5, 2007, security incident at Orlando International Airport (MCO). The breach involved two Comair Airline employees who successfully smuggled 14 firearms and 8 pounds of marijuana onboard a Delta Airlines commercial airplane bound for San Juan, PR (SJU). Additional objectives of the audit were to review TSA's current oversight of airport employees and the feasibility of 100 percent screening for airport employees attempting to gain access to an aircraft or the secured areas in an airport.

The OIG conducted its review between November 2007 and April 2008. To accomplish its objectives, the OIG interviewed and collected information from TSA Headquarters officials; MCO and SJU officials; the Greater Orlando Aviation Authority; Delta and Comair at MCO; the Freedom Center; union, airport, and airline industry officials; site visits to seven airports; U.S. Customs and Border Protection (CBP); and U.S. Immigration and Customs Enforcement (ICE). The OIG also evaluated TSA's current and former processes for screening airport employees at MCO.

The OIG investigation focused on three questions:

1) Did TSA policies cause MCO to be susceptible to security breaches, particularly involving the introduction of prohibited items into any secured areas of the airport?

2) What is the overall effectiveness of TSA's oversight of airport employees?

3) What is the feasibility of implementing 100 percent airport employee screening for individuals accessing an aircraft or the secured areas of an airport?

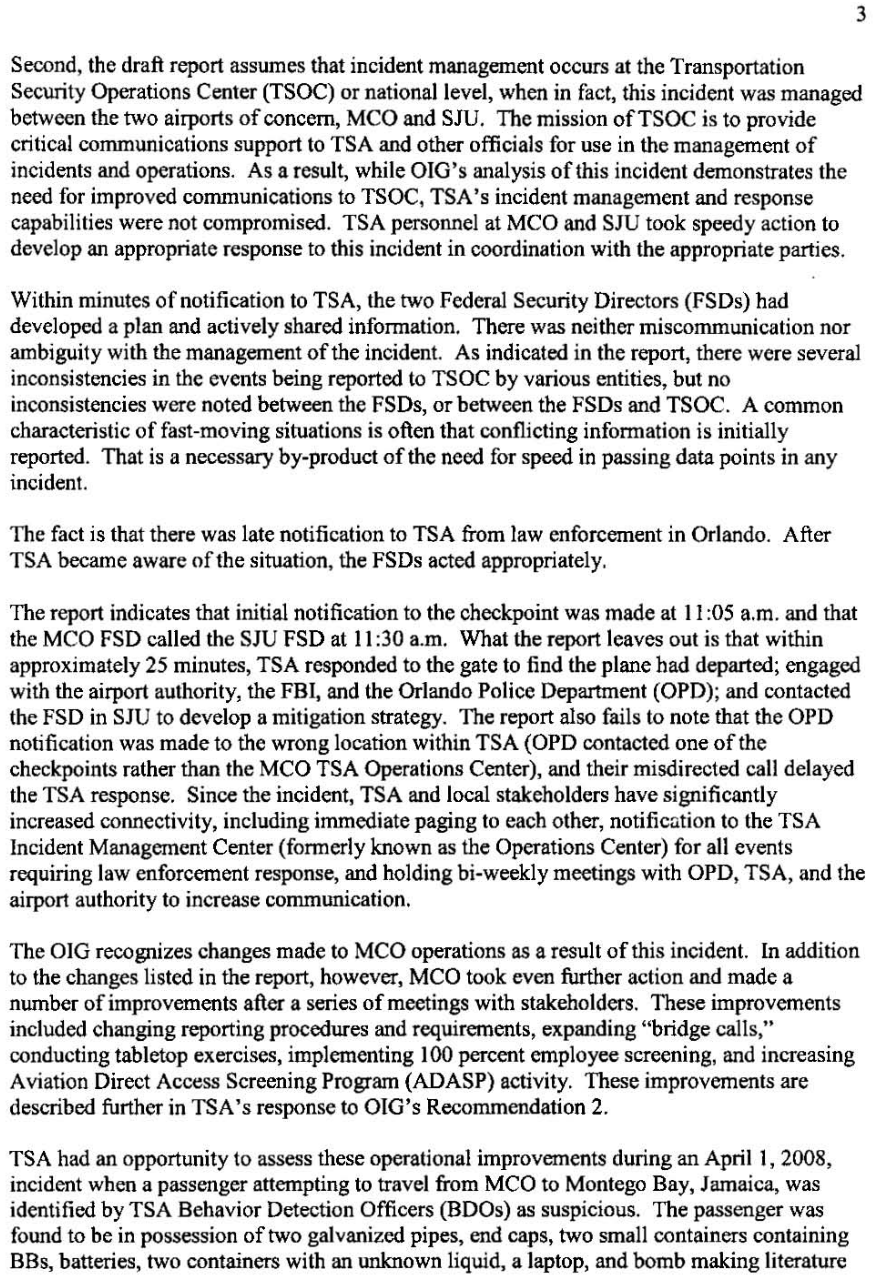
The OIG raised questions concerning TSA's incident management capabilities and regulatory framework governing the conduct of employees working at an airport. The OIG concluded that while the insider threat, which includes any current or former employee who has, or had, authorized access or knowledge about an organization's exploitable internal workings, remains a concern throughout the aviation community, it is unrealistic to assume that 100 percent airport employee screening would have prevented the March 5, 2007, incident at MCO. The OIG noted on page 39 of its draft report that:

> The concept of 100% airport employee screening is feasible. However, we do not believe it is realistic at this time. Regardless of the amount of funding, resources, and effort allocated toward this endeavor, vulnerabilities will persist. While the intelligence, screening, and law enforcement communities continue to make progress in addressing these vulnerabilities, 100% airport employee screening cannot entirely bridge existing gaps. As TSA changes its regulatory requirements, technology improves, and airports upgrade existing security measures, implementing this concept would be more realistic and should be revisited.

Discussion

While TSA appreciates the work OIG has done concerning this review, the draft report does not adequately or accurately reflect the events as they unfolded, or the subsequent actions taken. Therefore, TSA would like to provide the following clarification for several issues discussed in the report.

The comment on page 9 of the draft report, "TSA's inefficient handling of this incident raises questions about TSA's incident management capabilities and regulatory framework that governs the conduct of employees working at the airport," is not accurate. First, the incident in question was the subject of [redacted] into drug smuggling. At no time during the incident, or subsequent to it, was there a belief of a terrorism nexus with this incident. It is important to note that not all crimes committed on airport property are of interest to TSA from a counter-terrorism perspective. Furthermore, the initial report from OPD to TSA and Delta Airlines (Delta) stated the employee had "contraband" which both TSA and Delta initially believed meant drugs and likely resulted in the incorrect initial reporting. This incorrect reporting did not have any bearing on the actual response to the incident by local TSA authorities.



Second, the draft report assumes that incident management occurs at the Transportation Security Operations Center (TSOC) or national level, when in fact, this incident was managed between the two airports of concern, MCO and SJU. The mission of TSOC is to provide critical communications support to TSA and other officials for use in the management of incidents and operations. As a result, while OIG's analysis of this incident demonstrates the need for improved communications to TSOC, TSA's incident management and response capabilities were not compromised. TSA personnel at MCO and SJU took speedy action to develop an appropriate response to this incident in coordination with the appropriate parties.

Within minutes of notification to TSA, the two Federal Security Directors (FSDs) had developed a plan and actively shared information. There was neither miscommunication nor ambiguity with the management of the incident. As indicated in the report, there were several inconsistencies in the events being reported to TSOC by various entities, but no inconsistencies were noted between the FSDs, or between the FSDs and TSOC. A common characteristic of fast-moving situations is often that conflicting information is initially reported. That is a necessary by-product of the need for speed in passing data points in any incident.

The fact is that there was late notification to TSA from law enforcement in Orlando. After TSA became aware of the situation, the FSDs acted appropriately.

The report indicates that initial notification to the checkpoint was made at 11:05 a.m. and that the MCO FSD called the SJU FSD at 11:30 a.m. What the report leaves out is that within approximately 25 minutes, TSA responded to the gate to find the plane had departed; engaged with the airport authority, the FBI, and the Orlando Police Department (OPD); and contacted the FSD in SJU to develop a mitigation strategy. The report also fails to note that the OPD notification was made to the wrong location within TSA (OPD contacted one of the checkpoints rather than the MCO TSA Operations Center), and their misdirected call delayed the TSA response. Since the incident, TSA and local stakeholders have significantly increased connectivity, including immediate paging to each other, notification to the TSA Incident Management Center (formerly known as the Operations Center) for all events requiring law enforcement response, and holding bi-weekly meetings with OPD, TSA, and the airport authority to increase communication.

The OIG recognizes changes made to MCO operations as a result of this incident. In addition to the changes listed in the report, however, MCO took even further action and made a number of improvements after a series of meetings with stakeholders. These improvements included changing reporting procedures and requirements, expanding "bridge calls," conducting tabletop exercises, implementing 100 percent employee screening, and increasing Aviation Direct Access Screening Program (ADASP) activity. These improvements are described further in TSA's response to OIG's Recommendation 2.

TSA had an opportunity to assess these operational improvements during an April 1, 2008, incident when a passenger attempting to travel from MCO to Montego Bay, Jamaica, was identified by TSA Behavior Detection Officers (BDOs) as suspicious. The passenger was found to be in possession of two galvanized pipes, end caps, two small containers containing BBs, batteries, two containers with an unknown liquid, a laptop, and bomb making literature in his checked baggage. TSA immediately initiated a coordinated response involving TSA, the Orange County Bomb Squad, OPD, and the FBI's local Joint Terrorism Task Force (JTTF). The passenger was later arrested by the FBI on a charge of attempting to introduce an explosive or incendiary device on an aircraft in violation of section 46505 of title 49, United States Code. The TSOC was informed of the incident within ten minutes in order to evaluate a national response.

The OIG alleges that TSA made no effort to investigate the actions of Delta as they relate to this incident, which is incorrect. Following the events, TSA held discussions with Delta, and Delta stated that OPD reported that "contraband" was aboard the aircraft. After the individual was removed, Delta believed the illegal activity was removed from the aircraft. Delta reported that at no time did they believe there was a security nexus until they were notified by TSA and the aircraft was in the air.

The OIG further alleges that TSA never conducted any internal assessments to determine why inaccurate or timely information continued to circulate throughout the organization after 11:30 a.m. In addition to the actions taken subsequent to this incident that are reported in response to Recommendation 2, the MCO FSD discussed reporting issues, specifically regarding the Executive Daily Summary, with the Eastern Area Director and Director of the TSOC.

Finally, in the report's discussion about achieving an integrated, DHS-wide perspective on airport security, it should be noted that no other DHS component had jurisdiction in this case. CBP and ICE had no statutory authority in this instance and would not have had the legal basis to become involved in this case. Even if this would have been an international flight, they would not have been able to add any capability to the incident response, as the aircraft was in the air when DHS was notified. A Regional DHS Director would not have added additional capability to this response.

TSA generally concurs with your recommendations and has already taken steps to address several of them. The following are TSA's specific responses to those recommendations.

Transportation Security Administration (TSA) Response
Department of Homeland Security (DHS) Office of Inspector General (OIG) Draft Report:

TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening

Recommendation 1: Enact national security measures that ensure TSA has the opportunity to clear an aircraft for departure when law enforcement officers intervene prior to a scheduled departure.

TSA Concurs. TSA has adopted national security measures to ensure that TSA has the opportunity to clear an aircraft for departure when law enforcement officers intervene prior to a scheduled departure. These measures are outlined in a TSA/Federal Aviation Administration (FAA) joint operating procedures memorandum and a TSA-issued security directive to airport operators (attached).

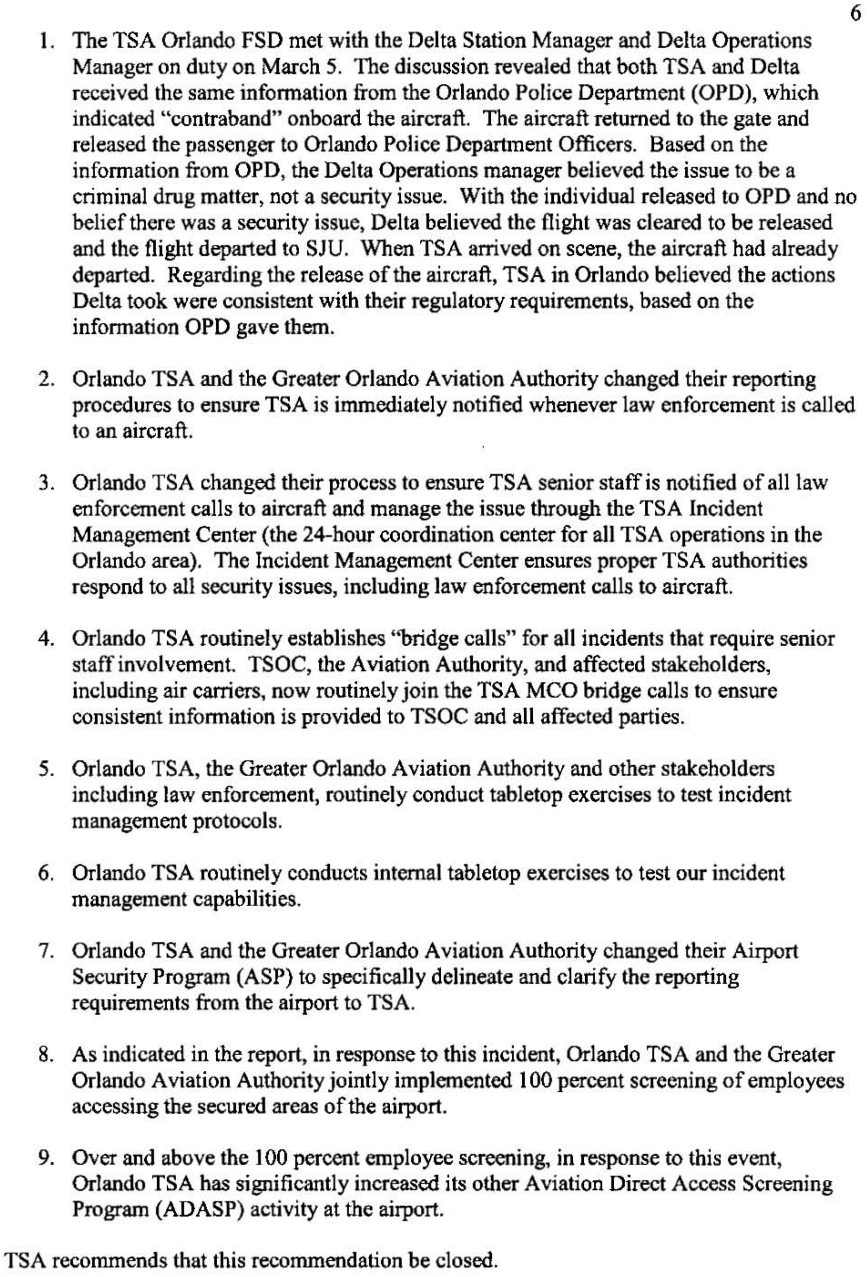
In October 2004, TSA and the FAA developed joint operating procedures to provide Air Traffic Managers (ATM) and Federal Security Directors (FSDs) with guidance for responding to both immediate and non-life threatening situations. The guidance states, in part, that, "if in the opinion of the FSD, there is an imminent and potentially life threatening security situation, the ATM, consistent with safety, will comply with the FSD's requested operational response."

TSA also issued a Security Directive (SD 1542-04-11B) on December 8, 2004, which requires airport operators to immediately notify FSDs of all incidents and suspicious activities that could affect the security of U.S. civil aviation. FSDs have the authority to hold a flight pending resolution of security concerns.

The Aircraft Operator Standard Security Program also requires aircraft operators to notify the Transportation Security Operations Center (TSOC) immediately of suspicious activities that could affect the security of aviation. If the aircraft is not airborne, the aircraft operator will normally inform the airport, and the airport will call in law enforcement. If the airport operator complies with the SD described above, the FSD may hold the flight. TSA is considering procedural changes to ensure that the FSD also receives timely notification of such reports.

Recommendation 2: Evaluate the March 5, 2007, incident at the Orlando International Airport in Florida, develop an assessment of Delta Airlines' role, and determine whether incident management protocols, oversight responsibilities, or training procedures need to be revised.

TSA Concurs With Comments. TSA appreciates OIG's recommendations on this subject and has taken significant action to review the March 5, 2007, incident and implement operational improvement. After the events of March 5, 2007, TSA and the stakeholders at the Orlando International Airport (MCO) held a series of meetings and made several improvements. TSA will review the following actions taken at MCO and will develop best practices to share with all FSDs and encourage their implementation at other airports. In some cases, other airports have already implemented similar procedures.



1. The TSA Orlando FSD met with the Delta Station Manager and Delta Operations Manager on duty on March 5. The discussion revealed that both TSA and Delta received the same information from the Orlando Police Department (OPD), which indicated "contraband" onboard the aircraft. The aircraft returned to the gate and released the passenger to Orlando Police Department Officers. Based on the information from OPD, the Delta Operations manager believed the issue to be a criminal drug matter, not a security issue. With the individual released to OPD and no belief there was a security issue, Delta believed the flight was cleared to be released and the flight departed to SJU. When TSA arrived on scene, the aircraft had already departed. Regarding the release of the aircraft, TSA in Orlando believed the actions Delta took were consistent with their regulatory requirements, based on the information OPD gave them.

2. Orlando TSA and the Greater Orlando Aviation Authority changed their reporting procedures to ensure TSA is immediately notified whenever law enforcement is called to an aircraft.

3. Orlando TSA changed their process to ensure TSA senior staff is notified of all law enforcement calls to aircraft and manage the issue through the TSA Incident Management Center (the 24-hour coordination center for all TSA operations in the Orlando area). The Incident Management Center ensures proper TSA authorities respond to all security issues, including law enforcement calls to aircraft.

4. Orlando TSA routinely establishes "bridge calls" for all incidents that require senior staff involvement. TSOC, the Aviation Authority, and affected stakeholders, including air carriers, now routinely join the TSA MCO bridge calls to ensure consistent information is provided to TSOC and all affected parties.

5. Orlando TSA, the Greater Orlando Aviation Authority and other stakeholders including law enforcement, routinely conduct tabletop exercises to test incident management protocols.

6. Orlando TSA routinely conducts internal tabletop exercises to test our incident management capabilities.

7. Orlando TSA and the Greater Orlando Aviation Authority changed their Airport Security Program (ASP) to specifically delineate and clarify the reporting requirements from the airport to TSA.

8. As indicated in the report, in response to this incident, Orlando TSA and the Greater Orlando Aviation Authority jointly implemented 100 percent screening of employees accessing the secured areas of the airport.

9. Over and above the 100 percent employee screening, in response to this event, Orlando TSA has significantly increased its other Aviation Direct Access Screening Program (ADASP) activity at the airport.

TSA recommends that this recommendation be closed.

Recommendation 3: Change the regulatory requirements to include provisions for mandating phased-in biometric access controls for airport operators, and recurrent criminal history and financial records check for Secure Identification Display Area badge employees.

TSA Concurs. TSA has initiated the process to include provisions for a phased-in biometric access control system for airport operators. TSA is working on standards for biometric access control systems and recurrent criminal history records check for employees with unescorted access to the Security Identification Display Area. TSA must resolve many technical and policy issues. As for financial records checks, TSA will take the recommendation into consideration.

Two recently issued documents provide a broad perspective of TSA's current thinking about biometric smart cards and their application at airport access control points. In May 2008, TSA released the *Aviation Credential Interoperability Solution (ACIS) Technical Specifications* to the airport operators and aircraft operators for review and comment. This document discusses many of the technical issues that TSA will consider in establishing standards. It focuses on the biometric credential and underlying processes, such as enrollment, vetting, and issuance of the credential.

In addition, an advisory committee sponsored by the FAA recently issued a document that may encourage the use of biometrics at airports and will be considered in the TSA standards. The Radio Technical Commission for Aeronautics, Inc.[1] (RTCA), with the participation of TSA, aviation industry representatives, airports, and security and IT consultants, recently updated its document that addresses standards for airport access control, specifically as they relate to biometrics. On June 25, 2008, the RTCA posted the updated version on its website, *RTCA DO 230-B Integrated Security System Standards for Airport Access Control*. The document aggregates industry best practices for the employment of perimeter security measures, including the use of biometric smart cards at access control points. It references the ACIS concept in relevant sections.

Furthermore, TSA completed the employee screening pilots at the seven airports as mandated in the *Consolidated Appropriations Act of 2008*. TSA and Homeland Security Institute (HSI), an independent contractor, will evaluate the result of the pilots and report back to Congress as mandated in the Act.

Recommendation 4: Apply effective and consistent Aviation Direct Access Screening Program policies and procedures at all airports.

[1] The RTCA website (www.rtca.org) identifies RTCA as a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management (CNS/ATM) system issues. RTCA also notes that it functions as a Federal Advisory Committee, and its recommendations are used by the FAA as the basis for policy, program, and regulatory decisions and by the private sector as the basis for development, investment, and other business decisions.

TSA Concurs. On March 19, 2007, and in response to the MCO incident, TSA implemented ADASP procedures for screening individuals and their accessible property at the boarding gate and visual inspections of aircraft. Shortly thereafter, on November 7, 2007, TSA implemented procedures to conduct [redacted] and at Direct Access Points (DAP). On May 5, 2007, TSA implemented additional procedures for conducting Liquid Container Screening. Each change to the screening procedures was accompanied by mandatory ADASP training, which must be completed before a Transportation Security Officer (TSO) is certified to conduct ADASP screening operations. To facilitate consistency in applying ADASP procedures, TSA established an ADASP Coordination Team in April 2007. Part of the team's responsibility is to respond to ADASP questions from the field. The questions and responses are made available to all TSOs. The Coordination Team also reviews the ADSAP standard operating procedures to determine whether revisions are necessary to clarify procedures.

TSA recommends that this recommendation be closed.

Recommendation 5: Establish an ADASP working group to consider policy and procedure changes based on an accumulation of best practices across the country.

TSA Concurs. TSA formed the Headquarters (HQ) ADASP Coordination Team in April 2007. This team consists of personnel from TSA's Procedures Division (part of the Office of Security Operations (OSO)), Special Screening Programs (part of OSO), Transportation Security Network Management, Office of Chief Counsel, and Office of Compliance (part of OSO). The team collaborates when changes to the ADSAP procedures are suggested, including at the conclusion of an ADASP Pilot or special operation, and when questions regarding ADASP procedures are received from the field. The HQ ADASP Coordination Team reviews the questions and provides clarification and guidance by posting the response on an electronic database accessible to all TSOs. The HQ ADASP Coordination Team meets regularly to consider possible ADASP procedural changes and also provides assistance regarding procedures when pilots are conducted.

TSA recommends that this recommendation be closed.

Recommendation 6: Establish an inter-component working group among U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and TSA, with the goal of piloting an integrated, DHS-wide operational concept at select airports.

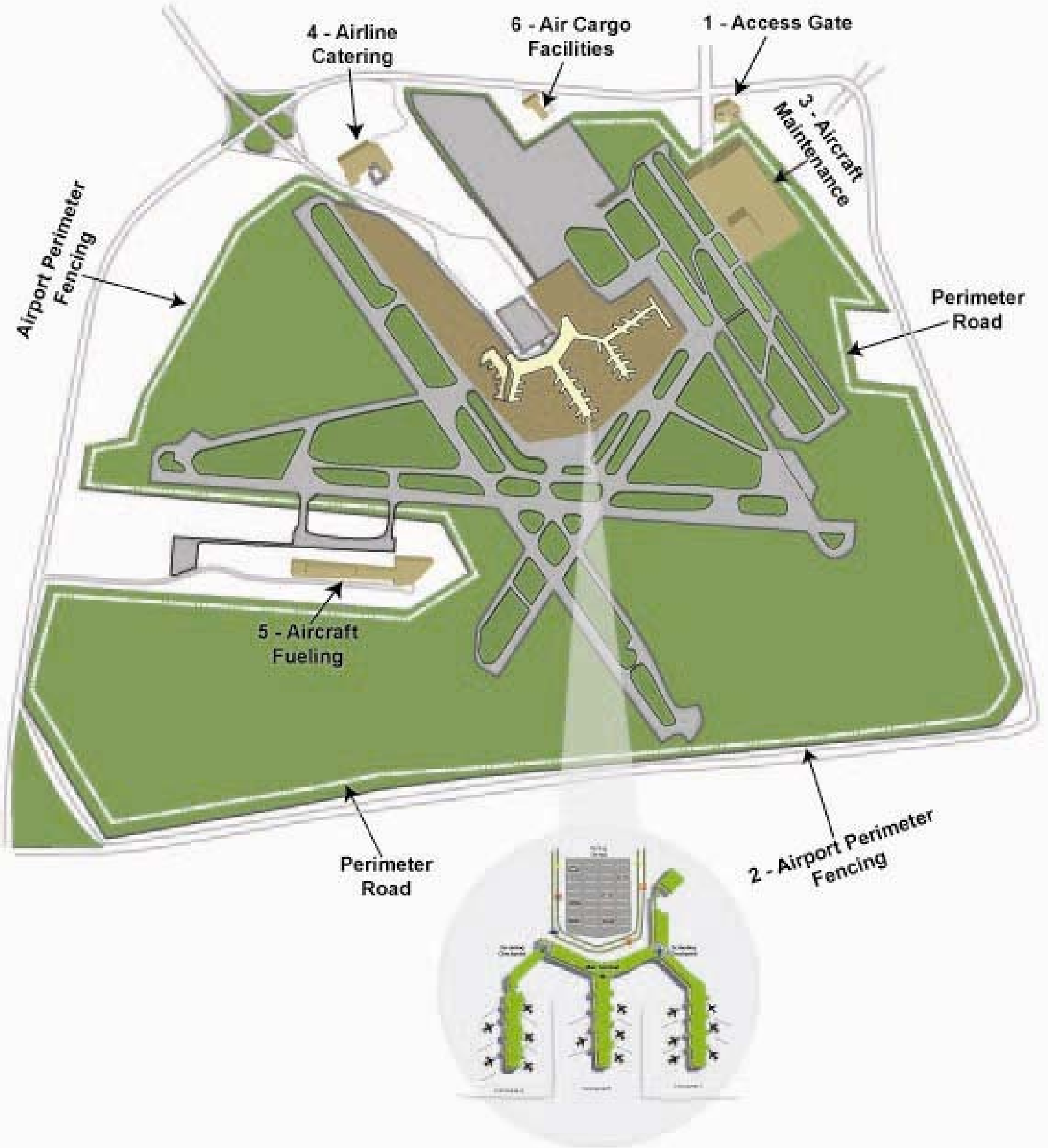
TSA Concurs. At airports with a combination of international and domestic operations, TSA already partners with CBP and ICE, as well as the Federal Bureau of Investigation (FBI), Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), U.S. Drug Enforcement Administration (DEA), and State, local, or airport police. These partnerships demonstrate an integrated DHS operational concept. TSA will coordinate with our colleagues within DHS to discuss the feasibility of establishing a DHS-wide pilot at select airports that have ports of entry.

Appendix C
TSA's List of Disqualifying Criminal Offenses (49 CFR § 1542.209 (d))

1. Forgery of certificates, false marking of aircraft, and other aircraft registration violations
2. Interference with air navigation
3. Improper transportation of hazardous material
4. Aircraft piracy
5. Interference with flight crew members or flight attendants
6. Commission of certain crimes aboard aircraft in flight
7. Carrying a weapon or explosive aboard aircraft
8. Conveying false information and threats
9. Aircraft piracy outside the special aircraft jurisdiction of the United States
10. Lighting violations involving transporting controlled substances
11. Unlawful entry into an aircraft or airport areas that serve air carriers or foreign air carriers contrary to established security requirements
12. Destruction of an aircraft or aircraft facility
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
    - ix. Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than one year
27. Violence at international airports
28. Conspiracy or attempt to commit any of the previously listed disqualifying criminal offenses

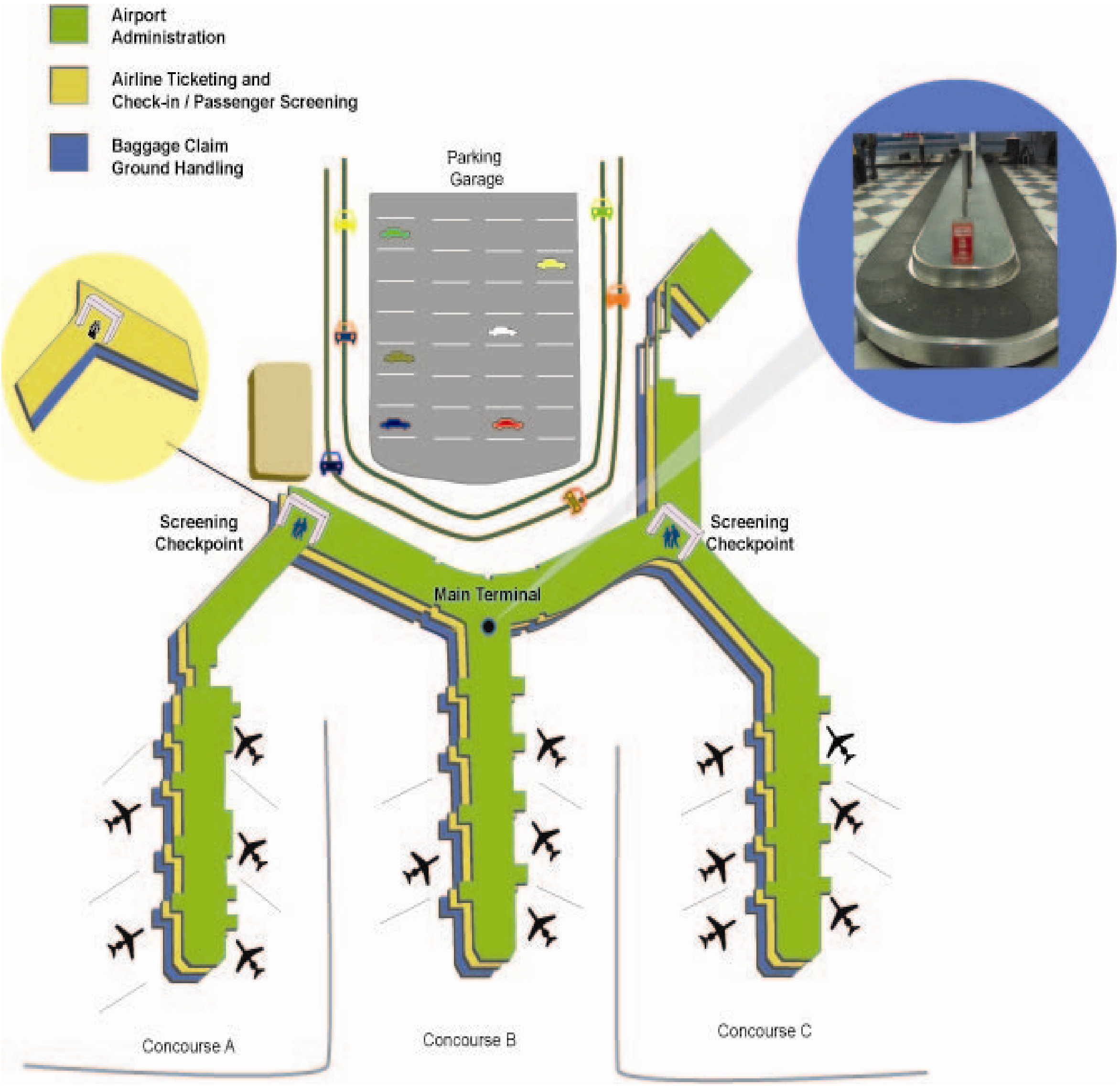
Appendix D
Airport Layout

Airport Layout



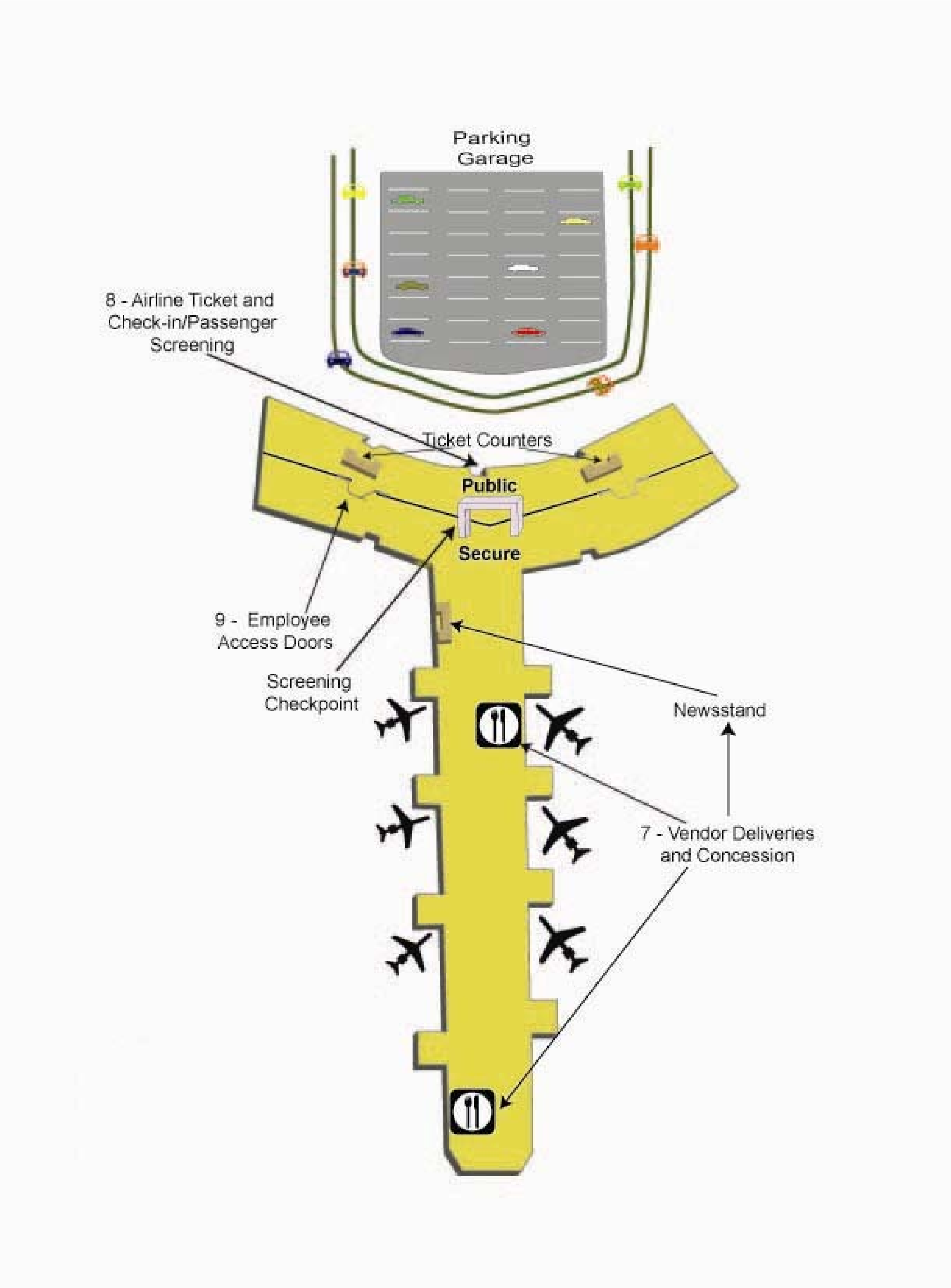
Appendix D
Airport Layout

Terminal View



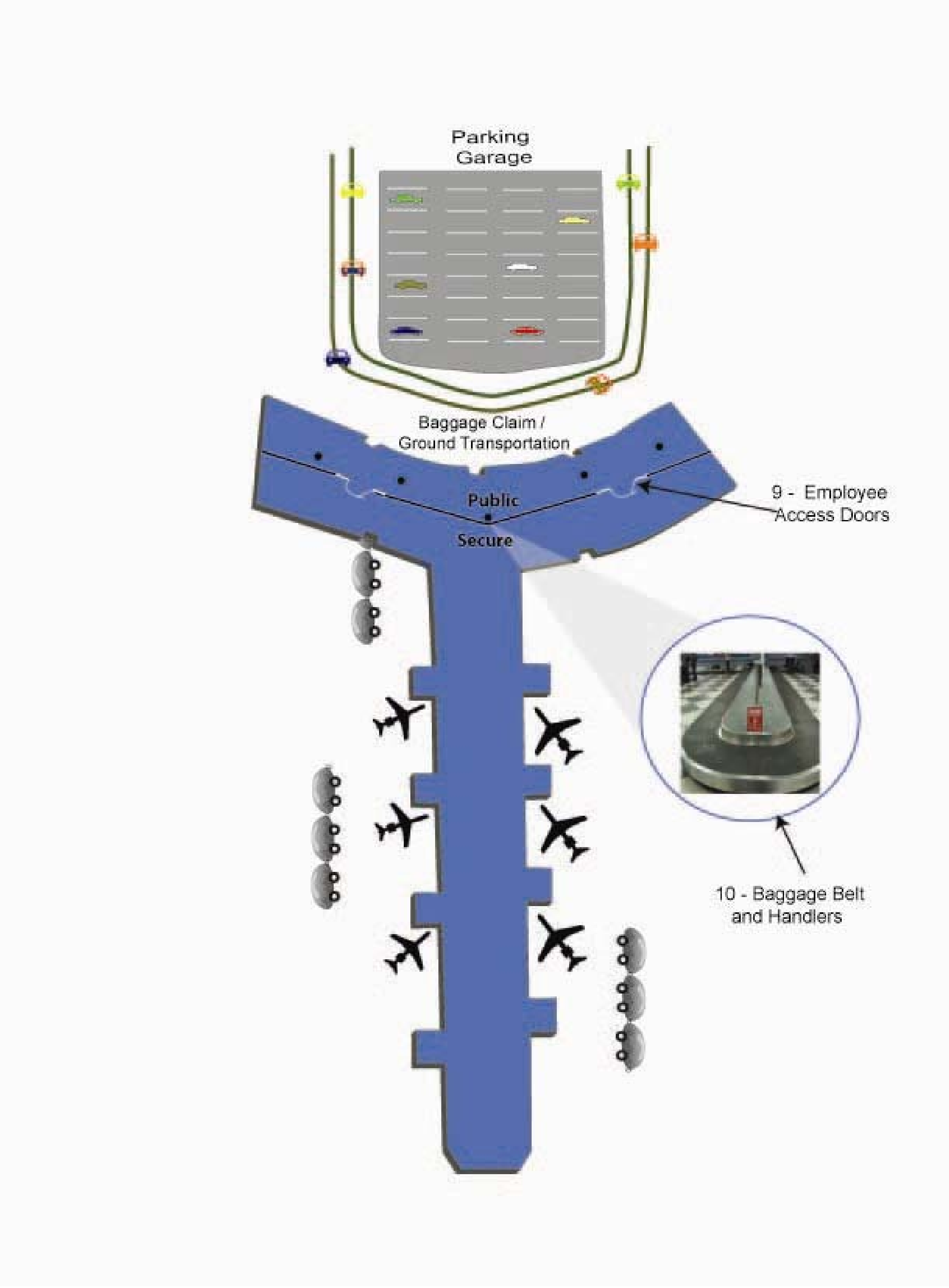
Appendix D
Airport Layout

Passenger Ticketing and Screening View


Parking Garage
8 - Airline Ticket and Check-in/Passenger Screening
Ticket Counters
Public
Secure
9 - Employee Access Doors
Screening Checkpoint
Newsstand
7 - Vendor Deliveries and Concession

Appendix D
Airport Layout

Baggage Claim and Ground Transportation View



Appendix E
Major Contributors to this Report

Marcia Moxey Hodges, Chief Inspector, Department of Homeland Security, Office of Inspector General, Office of Inspections

Angela Garvin, Senior Inspector, Department of Homeland Security, Office of Inspector General, Office of Inspections

Ryan Carr, Inspector, Department of Homeland Security, Office of Inspector General, Office of Inspections

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Policy
Assistant Secretary for Transportation Security Administration
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
TSA Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS Program 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) 254-4199, 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.