DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Review of Allegations Regarding San Francisco International Airport

Office of Audits

OIG-07-04

October 2006

Office of Inspector General

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

Homeland Security

October 26, 2006

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 responsibility to promote economy, efficiency, and effectiveness within the department.

This report assesses how security incidents have been identified and reported at San Francisco International Airport (SFO) and whether those procedures are consistent with Transportation Security Administration (TSA) policy. It also assesses whether and to what extent covert security testing was compromised at SFO. The report is based on interviews with employees and officials of relevant agencies and corporations and a review of applicable documents.

The recommendations contained in this report have been developed to the best knowledge available to us, and have been discussed in draft with appropriate management officials. 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
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

AFSD	Assistant Federal Security Director
ATO	Airport Task Order
ATSA	Aviation and Transportation Security Act
AVO	Aviation Operations Directives
BOA	Basic Ordering Agreement
CAS	Covenant Aviation Security
DFSD	Deputy Federal Security Director
DHS	Department of Homeland Security
FSD	Federal Security Director
OIAPR	Office of Internal Affairs and Program Review
OIG	Office of Inspector General
PP5	Private Screening Pilot Program
PARIS	Performance and Results Information System

Table of Contents/Abbreviations

PMIS	Performance Measurement Information System
SCC	Screening Control Center
SFO	San Francisco International Airport
SPP	Screening Partnership Program
TIP	Threat Image Projection
TSA	Transportation Security Administration
TSOC	Transportation Security Operations Center

OIG

Audit Report

Department of Homeland Security
Office of Inspector General

Executive Summary

This report presents the results of our review of allegations that Transportation Security Administration (TSA) officials at San Francisco International Airport (SFO) covered up known security breaches at SFO and compromised Office of Inspector General (OIG) covert security testing. We conducted this review at the request of TSA management, as a result of preliminary findings by TSA's Office of Internal Affairs and Program Review (OIAPR). Our objectives were to determine (1) whether TSA management at SFO complied with TSA policy and procedures for identifying and reporting security incidents; and (2) whether and to what extent covert security testing has been compromised at SFO and if so, who was responsible for those actions.

Generally, SFO management complied with TSA policy and procedures when identifying and reporting security incidents. However, we identified one uncontrolled security incident, in which SFO failed to report in TSA's Performance and Results Information System (PARIS). Although TSA management at SFO could not explain why the incident was not reported, we identified no evidence that management acted intentionally to cover up or misreport security incidents. We confirmed the allegation that TSA and Covenant Aviation Security (CAS) officials at SFO compromised OIG covert security testing between August 2003 and May 2004 by tracking testers throughout the airport via surveillance cameras and on foot, and then notifying screening personnel in advance of testers arriving at checkpoints. In May 2004, CAS management, along with TSA management at SFO, issued directives that all compromising activity surrounding covert security testing was to stop. We referred the matter of TSA's involvement in compromising covert security testing to our Office of Investigation.

We are recommending that TSA direct the Federal Security Director (FSD) at SFO to ensure that appropriate members of his staff are trained in and have a thorough knowledge of the guidelines for reporting security incidents to TSA headquarters through PARIS and the Transportation Security Operations Center (TSOC). Also, we recommend that TSA establish and promulgate policy to regulate its actions in response to authorized covert security testing of checkpoints. TSA concurred with one recommendation; partially concurred with the other, and has taken actions to resolve both.

Background

On November 19, 2001, the President signed the Aviation and Transportation Security Act (ATSA) that created TSA. ATSA, in part, required TSA to implement a two-year private security screening pilot program. On October 11, 2002, TSA awarded CAS a contract to provide security screening at SFO.

In November 2004, a CAS security screener at SFO sent a letter containing various allegations to CAS and TSA management. In January 2005, TSA's OIAPR investigated six allegations and determined that two of them had some merit. Specifically, (1) TSA officials were covering up known security breaches at SFO by classifying "serious breaches" as "mere incidents;" and (2) TSA and CAS officials were compromising OIG and OIAPR covert security tests by broadcasting tester descriptions and methodologies to all screening areas.

In February 2005, TSA management recommended that, due to the critical nature of OIAPR's investigation results, the allegations be referred to the OIG for review. As a result, OIAPR transferred all relevant working papers and statements collected during the course of its review to the OIG's Office of Audits.

TSA's *AVO 400.18.1-1B: Reporting Security Incidents* directs Federal Security Directors (FSDs) or their designees to report all security incidents, as defined within this directive, that occur at their airports. These reports are to be submitted to TSA headquarters through PARIS.[1] To ensure that consistent, accurate, and timely information is reported, each FSD is directed to instruct the appropriate staff members to collect the information required under this AVO. The FSD or his/her designee is directed to review and approve each report within 24 hours and submit it to TSA headquarters through PARIS.

This AVO contains 28 types of security incidents. Each incident type is defined and has minimal examples to assist in categorizing the incidents. One such category is a breach of security checkpoint. TSA's AVO 400.50.1-25: *Security Breach at Passenger Screening Checkpoint: Revised Guidance* contains the definition of what constitutes a security breach, procedures for managing the response to a potential or actual security breach, training for those involved, and coordination with local authorities. This AVO provides the following definitions:

- *Security Breach* - when a person enters the sterile area without submitting to all screening and inspection of his or her person and

[1] PARIS is a TSA database application that tracks information about security incidents at the nation's airports. In addition to the PARIS reporting, some security incidents in this directive are marked to indicate that they must also be reported immediately by telephone to TSOC.

accessible property in accordance with the procedures being applied to control access to the sterile area.

- *Uncontained Security Breach* - situation where security personnel and law enforcement are not able to continuously monitor and respond to the uncleared person or item in the sterile area.

FSDs and their staffs must pay particularly close attention to the definitions of the incident type to ensure consistent reporting nationally. Consistent, accurate, and timely reporting on the number and nature of security incidents is important because TSA uses this information in lawsuits, civil enforcement actions, and criminal prosecutions, as well as to disseminate information to other TSA components. Reporting security incidents also serves to:

- Alert TSA management to potentially dangerous or high-profile events requiring crisis management or responses to media or congressional inquiries;
- Allow trend and link analyses of security-related incidents at each airport, within each TSA area and nationwide; and
- Identify new security threats, problem passengers, suspicious activities, or new ways to artfully conceal prohibited items.

Results of Review

SFO Management Generally Complied With TSA Procedures When Identifying and Reporting Security Incidents

SFO management generally complied with TSA policy and procedures when identifying and reporting security incidents. However, the guidelines and definitions in AVO *400.18.1-1B: Reporting Security Incidents,* dated May 12, 2004, are broad in scope and allow FSDs flexibility in categorizing security incidents and the resultant reporting. Also, we determined that only one of the five incidents which OIAPR determined to be a security incident in their investigation was actually a reportable security incident, and should have been reported to TSA headquarters through PARIS.

TSA Incident Identification and Reporting Guidance is Subject to Interpretation

According to AVO *400.18.1-1B,* all FSDs or their designees are required to report all security incidents that occur at their airports within 24 hours through PARIS. Additionally, uncontained security breaches must be reported immediately by telephone to the TSOC.[2] All FSDs or their designees must review and approve PARIS reports before they are submitted. FSDs and their staffs are directed to pay particularly close attention to the definitions of the incident type to ensure consistent reporting nationally.

This AVO identifies 28 types of security incidents. Within each incident type, there is a definition and minimal examples to assist in categorizing the incidents. The definitions of some security incident types are broad and allow for a degree of flexibility by the FSD. However, this broad scope means that TSA management at SFO, or any airport, is unable to be absolute in its determination of the type of security incident represented by the event and how the incident should be reported. For example, *Breach of Security Checkpoint* is defined as an incident in which an individual breaches a security checkpoint, whether intentionally or inadvertently, without proper screening. *Improper or No Screening* is defined as incidents involving a screener who fails to screen a passenger or does so improperly. If a passenger sets off the alarm and the screener does not resolve the alarm, the question becomes which category applies: a *Breach of Security Checkpoint* based on a passenger inadvertently breaching security without proper screening; or, *Improper or No Screening* as screener error for failure to resolve the alarm? According to TSA management, this results in a wide disparity in reporting among airports.

[2] The TSOC is TSA's single point of contact for security-related operations, incidents, or crises in aviation and all land modes of transportation. An uncontained security breach occurs when an individual passes through a security checkpoint without proper screening, whether intentionally or inadvertently, where visual control has been lost.

After OIAPR's review, which focused in part on the reporting of security incidents at SFO, the SFO Deputy Federal Security Director (DFSD) solicited the opinion of an Aviation Operations subject matter expert at TSA headquarters to confirm interpretation of the AVO. The DFSD found that SFO's interpretation was in agreement with TSA's expert opinion regarding the identification and reporting of security breaches to the TSOC. Following this inquiry, the DFSD sent a memorandum to Aviation Operations at TSA headquarters to formally request clarification of the definition and intent of the AVO for reporting security incidents. Aviation Operations management officials stated they would develop a decision matrix of various breach scenarios to assess the risks associated with each of the scenarios and identify appropriate responses. This matrix will assist FSDs in being able to determine what should and should not be reported as a breach.

Screening and Regulatory Divisions are Tasked with Identifying and Reporting Security Incidents at SFO

AVO *400.18.1-1B* also directs FSDs to instruct the appropriate staff members to collect the information required to satisfy the reporting requirement under this AVO, according to the incident type. Since the screening function at SFO was federalized in 2002, the Screening Division has been tasked with responding to and collecting the information surrounding security incidents. However, the various duties associated with preparing the template used to report security incidents in PARIS have fluctuated between the Screening Division and the Regulatory Division. According to TSA management, the responsibility for compiling the information needed to complete the template, which includes categorizing the incident, inherently lies with the Regulatory Division. The Regulatory Division is responsible for all matters concerning enforcement and compliance with security directives pertaining to airport and aviation security. However, when the screening function at SFO became a federal responsibility, the Regulatory Division did not have sufficient staff to handle all of the reporting responsibilities associated with the volume of reportable security incidents. Therefore, the Screening Division was tasked with a major share of these time-consuming responsibilities.

The Regulatory Division has always been responsible for reviewing, approving, and submitting security incident reports to PARIS and the TSOC when applicable. In August 2004, following an increase in staffing, the preparation of the reporting template, which includes identifying incident types, was shifted to the Regulatory Division.

In June 2005, preparation of the PARIS reporting template on routine prohibited items such as box cutters and knives with blades three inches or longer, was shifted back to the Screening Division at SFO. This occurred when the SFO DFSD became aware, in January 2005, that SFO was not

properly reporting in PARIS a portion of the prohibited items confiscated, namely box cutters and knives with blades three inches or longer, as required in the AVO. SFO had been properly reporting these items in the Performance Measurement Information System (PMIS). The number of items confiscated in this category has caused a large increase in staff-hours to report them in PARIS. As a result, SFO shifted this specific incident responsibility to the Screening Division. The remainder of the PARIS reporting responsibilities remains with the Regulatory Division.

One Security Incident in OIAPR's Sampling Was Not Reported in PARIS

In its initial investigation, OIAPR found that five incidents recorded in CAS *Safeskies* (an online journal), within a five month sampling period from June 2004 to October 2004, appeared to meet the definition of a security breach as set forth in A*VO 400.50.1-25* and had not been reported in PARIS. However, we determined that only one of these incidents should have been reported to TSA headquarters through PARIS.

Safeskies is an online journal maintained by CAS to document certain events, including security incidents, occurring at SFO. This online journal is maintained by staff in the Screening Control Center (SCC) at SFO to provide CAS corporate management in Illinois access to information regarding events as they occur at SFO. *Safeskies* entries cannot be edited, and sometimes contain only initial descriptions of incidents. The entries do not include follow-on measures used in resolving the incident.

TSA management at SFO is responsible for all operational reporting to TSA headquarters. They use their internal system for collecting information at the screening checkpoints on security incidents. Under this system, the FSD and the DFSD are always briefed on significant security incidents. Each Screening and Operations Manager prepares a daily log detailing all important activities, including security incidents, occurring on their shift. The daily logs from each terminal are compiled into a document known as the Daily Incident Report.

These reports are delivered every morning to all TSA senior management and key personnel at SFO for their review. This review provides an opportunity to correct any incident identification errors or notification oversights made by the Screening Division and the Regulatory Division. Since a security screener made the allegations of misreporting in November 2004, implementation of reporting checklists and emphasis on closer reviews has reinforced this internal review process.

We determined that the five security incidents identified by OIAPR in their initial investigation, as recorded in CAS *Safeskies* but not reported in PARIS,

were also recorded in the Screening Division's Daily Incident Reports. We reviewed the five incidents as detailed in these Daily Incidents Reports and determined that four of the five security incidents were not reportable security incidents within the definition provided in *AVO 400.18.1-1B.* One security incident was an uncontained security breach, as the result of a screener failing to complete secondary screening. As such, it should have been reported to TSA headquarters through PARIS and to the TSOC.

After reviewing the videotape, at or near the time of the incident, two senior TSA Screening Division management officials and the responding TSA Screening Manager identified this one security incident as an uncontained security breach, and therefore, reportable under the AVO. However, the incident was not reported to TSA headquarters through PARIS or by phone to the TSOC. Screening Division management could not explain why the incident was not reported, but suggested that it may have been an administrative oversight. We did not identify any evidence to suggest that any Screening Division personnel acted to withhold notification of this incident intentionally. However, we determined that, based on the facts surrounding the incident, it should have been reported to TSA headquarters through PARIS and to the TSOC. In addition, as the senior responding official, the Assistant Federal Security Director (AFSD) for Screening had the specific responsibility for ensuring that the incident was reported. The FSD agreed with this determination.

Recommendation 1: We recommend that TSA direct the SFO FSD to ensure that appropriate members of its staff are trained in and have a thorough knowledge of the guidelines for reporting security incidents to TSA headquarters through PARIS and the TSOC.

Management Comments and OIG Analysis

TSA concurred with our recommendation. The FSD at SFO issued a local directive in November 2005 detailing the process for reporting security incidents at SFO, and the training program established to ensure that all staff personnel have a thorough knowledge of reporting requirements through both PARIS and the TSOC.

In addition, a TSA Operations Directive issued in August 2005 provides the requirements for reporting security incidents to the TSOC. Both directives are provided to all TSA and contractor management personnel during new-hire training.

We have determined that the actions TSA has taken are responsive to our recommendation that SFO staff be trained in, and have a thorough knowledge of, the guidelines for reporting security incidents to TSA headquarters through

both PARIS and the TSOC. Therefore this recommendation is resolved and closed.

Covert Security Testing at SFO Was Compromised

Under the direction of TSA and CAS management at SFO, SCC personnel compromised OIG and OIAPR covert security testing between August 2003 and May 2004 by tracking testers throughout the airport via surveillance cameras and on foot. Then they notified screening personnel in advance when a tester was approaching a checkpoint and provided their descriptions. Broadcasting descriptions and locations of testers to screening checkpoints impedes the testing and distorts the results of OIG audits. As a result, the need for changes in policies, additional training of screeners, and additional staffing as well as equipment inadequacies may not be revealed. At the end of our fieldwork, TSA had not published guidance to regulate how TSA airport management and screening personnel should respond to authorized covert security testing of any airport screening procedures or facilities. We referred the matter of TSA's SFO management involvement in compromising covert security testing to our Office of Investigation. A chronology of events, including covert security testing dates, occurring at SFO is provided as *Appendix C.*

During the period August 2003 to January 2005, TSA and CAS officials at SFO notified CAS personnel in the SCC of the start of covert security testing and directed them to notify checkpoint-screening supervisors that covert security testing was beginning. The DFSD established this practice after local news media personnel conducted unauthorized security tests at SFO's passenger screening checkpoints on February 26, 2003. The news media conducted these tests following a serious breach at SFO, which occurred February 6, 2003, and resulted in the evacuation of SFO's largest terminal. This affected more than 40 scheduled flights at an estimated cost of $800,000.

According to TSA SFO management, they wanted the SCC to exercise command and control over the checkpoints to provide immediate reaction and communication for breach control. Therefore, management directed that the cameras be trained on testers. In this process, TSA SFO management encouraged SCC controllers to use the cameras in such a way as to allow them to maintain visual contact from one surveillance area to next. For example, tracking of a subject is accomplished by switching from camera to camera by typing in the number of the camera in the next area. The SCC controllers must know the cameras by number and which areas they control to track a subject quickly.

When necessary, they are able to pull a videotape of an incident and have it ready for viewing by TSA SFO management within approximately two minutes.

In addition to tracking testers by CCTV, the SCC broadcasted descriptions and locations of testers to the checkpoints to assist the supervisors in identifying testers and to facilitate passing the covert penetration tests. The ability to broadcast this information was made possible by the extensive CCTV network available in the SCC at SFO.

SFO TSA management stated that they did not instruct CAS personnel to broadcast descriptions of testers, test methodologies, or locations of testers to the checkpoints. They stated that if this was done, it was the sole work of CAS employees, without any input from SFO TSA management. However, CAS officials and personnel provided evidence that the verbal directives to broadcast descriptions and locations of testers came from a member of SFO TSA management.

The advance notification regarding locations and descriptions of covert security testers continued until May 2004, when a CAS employee in the SCC refused to provide the descriptions and locations of testers and urged CAS management to intervene. CAS management then directed its personnel to cease all such compromising activity immediately. Senior CAS officials also secured TSA management's agreement to ensure that all compromising activity by TSA personnel was stopped.

However, notification of checkpoint supervisors of the start of covert security testers continued until January 2005. After the January 2005 tests by the OIG, the DFSD established a new protocol regarding SFO's response to covert security testing. Under this new protocol, TSA will inform the SCC when covert security testing is beginning; however, the SCC is prohibited from notifying the checkpoint screening supervisors that covert testing has begun.

Recommendation 2: We recommend that TSA establish policy to clarify TSA airport management and airport screening contractors' interaction with covert security testers.

Management Comments and OIG Analysis

TSA concurred in part with our recommendation. TSA believes that there is already policy in place to address the improper dissemination of official and sensitive information, which covers covert testing. A Human Resources Management Policy Letter provides the means to hold FSDs and other TSA personnel accountable for disclosing information about covert testing at an airport.

Because of SFO's unusual nature in having a contractor screening force and a sophisticated camera surveillance system, TSA and the contractor issued directives in May 2004 to stop all activity that could compromise the integrity

of covert security testing. TSA management at SFO issued another protocol in January 2005 that prohibits any notification to screening checkpoints that covert testing is being conducted.

We accept TSA's response to our recommendation and consider the recommendation resolved and closed.

Appendix A
Purpose, Scope and Methodology

We conducted this review at the request of TSA management, in response to allegations related to the reporting of security incidents, and actions taken to compromise OIG covert testing at San Francisco International Airport.

The objectives of the audit were to:

- Determine how security incidents are identified and reported at SFO and whether those procedures are consistent with TSA policy.
- Determine whether and to what extent covert security testing has been compromised at SFO and identify who was involved in these actions.

To accomplish our review, we conducted fieldwork at TSA headquarters in Arlington, Virginia, and at San Francisco International Airport and their off-site facilities in Southern San Francisco, California. We reviewed TSA's Aviation Operations Directives, Screening Checkpoint Standard Operating Procedures, and other relevant documentation pertaining to the identification and reporting of security incidents and the covert security testing process. We also received a briefing from the OIAPR investigative team to obtain their insights and comments regarding the allegations.

To obtain a thorough understanding of security incidents and covert security testing policies and procedures, we interviewed key TSA officials, including the Acting Deputy Assistant Secretary; the Assistant Administrator of Aviation Operations; the Program Executive, Screening Partnership Program; Program Analyst, Screening Partnership Program; Chief of Staff, Human Resources; Manager, Screening Outreach Programs, Office of Aviation Programs; and members of the OIAPR review team. At SFO, we interviewed the TSA Western Area Director and FSD; Deputy FSD; Director, Western Area Staff; Assistant FSD, Screening; Deputy Assistant FSD, Screening; Assistant FSD, Regulatory; Deputy Assistant FSD Regulatory; TSA Security Engineer; Aviation Security Inspectors; Screening Managers, and other TSA staff.

At SFO, we also interviewed key CAS officials, including the President; Executive Vice President; Vice President and General Manager; Vice President, Human Resources; Director of Operations; Deputy Director of Operations; Director of Training; Terminal Manager; SCC Supervisors; a Customer Service Specialist; Checkpoint Screening Supervisors; and other CAS staff.

We analyzed work papers and other relevant documents transferred from OIAPR. We toured and observed various terminals, screening checkpoints, and the SCC at SFO.

Appendix A
Purpose, Scope and Methodology

We conducted fieldwork between May 2005 and October 2005 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards. A listing of the major contributors to this report is included in *Appendix C.*

Appendix B
Management Comments to the Draft Report

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

JUL 21 2006

Transportation Security Administration

INFORMATION

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

FROM: Robert D. Jamison
Deputy Assistant Secretary

SUBJECT: Transportation Security Administration (TSA) Response Department of Homeland Security (DHS) Office of Inspector General (OIG) Draft Report "Review of Allegations Regarding San Francisco International Airport," May 2006

Purpose

This memorandum is TSA's formal agency response to the DHS OIG draft report, "Review of Allegations Regarding San Francisco International Airport," May 2006. TSA appreciates the work you have done to highlight areas for improvement with policy and procedures at San Francisco International Airport (SFO). We strongly believe that the implementation of the recommendations will lead to more effective covert testing programs for SFO and assist TSA and Covenant Aviation Security (CAS) in better Performance and Results Information System (PARIS) reporting to TSA Headquarters and the Transportation Security Operations Center (TSOC).

Background

The report states that during a 5-month sampling period SFO management failed to report one uncontrolled security incident in which a screener failed to perform secondary screening. Additionally, the report states that TSA and CAS officials at SFO compromised Office of Inspector General (OIG) and Office of Inspection (OI) (formerly Office of Internal Affairs and Program Review) covert testing between August 2003 and May 2004 by tracking testers throughout the airport via closed circuit television and on foot, notifying screening personnel in advance of testers arriving at their checkpoints.

Discussion

The Federal Security Director (FSD) at SFO has initiated a training program for staff personnel to ensure proper reporting of all security related incidents to TSA Headquarters and TSOC via PARIS. Further, in December 2005, the Deputy Federal Security Director (DFSD) at SFO established a new protocol regarding SFO response to covert security testing. Under this new protocol, TSA will inform the Screening Control Center (SCC) at the airport when covert testing is beginning; however, the SCC is prohibited from notifying the checkpoints' screening supervisors that covert testing has begun.

Our plans to correct the weaknesses noted in your report are in the attached TSA response. We strongly believe that these new protocols will eliminate any confusion with PARIS reporting on security incidents, and allow for a more effective covert testing program. Once again, TSA values the work the OIG is doing in this area and looks forward to continued communication in the future.

Attachment

Appendix B
Management Comments to the Draft Report

Transportation Security Administration (TSA) Response
Department of Homeland Security (DHS) Office of Inspector General (OIG) Draft Report
"Review of Allegations Regarding San Francisco International Airport," May 2006

Recommendation 1: TSA direct the SFO FSD to ensure that appropriate members of its staff are trained in and have a thorough knowledge of the guidelines for reporting security incidents to TSA headquarters through PARIS and TSOC.

TSA Concurs. The SFO Federal Security Director (FSD) has initiated a training program for staff personnel to ensure that they have a thorough knowledge of guidelines for reporting security incidents to TSA headquarters through PARIS and the Transportation Security Operations Center (TSOC). The training for reporting Security Incidents at SFO is covered under SFO 001-06 FSD Directive. The Directive was put in place on November 9, 2005, and covers reporting security incidents for PARIS and TSOC reporting. Additionally, TSA Operations Directive OD-400-18-2A (attached), effective August 26, 2005, covers reporting security incidents to TSOC. Both directives are provided to all TSA and contractor management during new hire training. Read and Acknowledge signature sheets are signed by all new hires for Aviation Security Inspectors, Covenant Aviation Security (CAS) Operations Management and Screening Manager positions. Training and compliance is accomplished through self study and audited per incident by TSA SFO management for accuracy. Compliance and accuracy are maintained by quality review of all reported incidents. The FSD directive is unique to SFO, and the TSOC reporting directive applies nationally for all airports.

Recommendation 2: TSA establish policy to clarify TSA airport management and airport screening contractors' interaction with covert security testers.

TSA Concurs in Part. TSA believes that there is already policy in place to address the improper dissemination of official and sensitive information, such as the fact that covert testing is being conducted at an airport. Human Resources Management (HRM) Policy Letter 735-1, titled "Interim Policy on Employee Responsibilities and Conduct," prescribes that "employees shall not: a. Divulge any official information obtained through or in connection with their government employment to any unauthorized person," and "b. Release any official information in advance of the time prescribed for its authorized issuance." HRM 735-1 provides the means to hold FSDs and other TSA personnel accountable for disclosing information about covert testing at an airport.

Recognizing the unique circumstances at SFO (e.g., a contractor screening force and a highly sophisticated closed circuit television system), in May 2004, TSA and CAS management at the airport issued directives that all compromising activity surrounding covert security testing was to stop. In January 2005, TSA management at SFO issued a new protocol regarding covert security testing. This protocol prohibits any notification to screening checkpoints of the start of covert security testing. In addition, the SFO FSD and DFSD met with TSA and CAS management staff to reinforce the fact that no notice or communication will be given to any person or group that

would allow prior knowledge of any covert testing being conducted by any authorized inspection team. Further, it was communicated that the AFSD-Screening or other parties were not authorized to change established policy without written approval from the FSD.

The subsequent FSD guidance for any type of covert testing prohibits alerts, communication, or notification of any kind that would compromise the covert testing. The FSD receives a call from the Team Leader from OIG or OI at the time covert testing commences; the FSD does not inform any other individuals at SFO that testing is underway to further protect the covert aspect of the test. All command and communication are in compliance with this FSD directive and all new hires are appraised of this requirement. Although the guidance is specific to SFO, it is consistent with the practices followed by OI in its covert testing protocols nationwide.

Appendix C
Chronology of Events

The following is a chronology of events related to covert security testing conducted at SFO by OIG and OIAPR testers.

Nov. 19, 2001	Public Law 107-71 creates TSA and requires a pilot program where the screening of passengers and property will be performed by private screening parties.
Jun. 18, 2002	TSA announces that five airports would be participating in the pilot program.
Oct. 10-11, 2002	TSA awards contracts for the Private Screening Pilot Program. Covenant Aviation Security received contract for airport at San Francisco, CA.
Nov. 19, 2002	Start of pilot program screening for passengers at airports.
Feb. 6, 2003	Security Breach, Terminal 3
Feb. 26, 2003	ABC News Media testing
Mar. 17-18, 2003	OIAPR Testing
Mar.-Apr. 2003	Screening Control Center with CCTV enhanced
Aug. 20-22, 2003	DHS-OIG Testing
Sept. 8-9, 2003	OIAPR Testing
Sept. 22, 25, 2003	OIAPR Testing
May 17-18, 2004	OIAPR Testing
Aug. 30, 2004	OIAPR Testing
Sept. 13, 2004	OIAPR Testing
Nov. 22, 2004	Screener's letter of allegations received
Nov. 24, 2004	President, CAS, letter to FSD, SFO (regarding ceasing all compromising activity)
Jan. 12-14, 2005	DHS-OIG Testing
Feb. 18, 2005	Screener files Wrongful Firing Lawsuit

Appendix D
Major Contributors to this Report

Alexander Best, Director, Transportation Security Audit Division
James Yeager, Audit Manager
Leigh Johnson-Steele, Auditor-In-Charge
Gary Alvino, Program Analyst

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Assistant Secretary for Policy
Assistant Secretary for Legislative and Intergovernmental Affairs
Assistant Secretary for Public Affairs
DHS GAO/OIG Liaison
DHS OIG Liaison, TSA
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528, fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller**.**