Department of Homeland Security
Office of Inspector General

Transportation Security Administration's Known Shipper Program

(REDACTED)

OIG-09-35

March 2009

Office of Inspector General

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

Homeland Security

March 5, 2009

Preface

The Department of Homeland Security, Office of Inspector General, was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the effectiveness of the Transportation Security Administration's Known Shipper Program. It is based on interviews with employees and officials of the Transportation Security Administration, direct observation, and a review of applicable documents.

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

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

DHS	Department of Homeland Security
KSDB	Known Shipper Database
KSMS	Known Shipper Management System
KSP	Known Shipper Program
TSA	Transportation Security Administration

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

The Transportation Security Administration is responsible for overseeing aviation security and ensuring the safety of the air traveling public. This includes the screening of all passengers and their personal property, as well as approximately 13,000 tons of cargo transported on passenger planes each day. The agency requires each regulated entity, such as an air carrier or freight forwarder, to ensure a shipper is known before accepting its cargo for transport on passenger aircraft.

The Transportation Security Administration is developing the Known Shipper Management System, which is an automated process for verifying the validity and integrity of shippers. The agency plans to make this the primary method for making shippers known; however, it must resolve challenges in the development and deployment of the system, including technical problems and policy issues. The other two methods available to verify a known shipper are manual procedures and the Known Shipper Database. These methods do not provide assurances that only known shipper cargo is transported on passenger aircraft. The agency's criteria and guidance for evaluating a shipper are unclear and subject to interpretation, increasing the risk that shippers may be improperly classified as known. The Transportation Security Administration's inspection and testing activities do not provide assurances that regulated entities are complying with the program's vetting requirements.

We are making six recommendations to the Assistant Secretary of the Transportation Security Administration to strengthen the controls and oversight of the Known Shipper Program. The agency generally concurred with our recommendations.

Background

The *Aviation and Transportation Security Act of 2001* requires the screening of all passengers and property transported on passenger planes. The Act gives the Transportation Security Administration (TSA) responsibility for overseeing aviation security and ensuring the safety of the air-traveling public. TSA continues to improve air cargo security using a risk-based, layered approach to enhance security without impeding the flow of commerce.

The Federal Aviation Administration created the Known Shipper Program (KSP) before the September 2001 terrorist attacks and the creation of the Department of Homeland Security. The KSP is one of TSA's key components for strengthening air cargo security. The program establishes procedures for differentiating between shippers that are known and unknown for air carriers and indirect air carriers who tender cargo for air transportation. Title 49 of the Code of Federal Regulation provides that, with limited exceptions, domestic and foreign passenger aircraft operators, all-cargo aircraft carriers, or indirect air carriers, also known as freight forwarders, operating under an approved TSA Standard Security Program may tender cargo for transport on passenger aircraft only from shippers that are verified as known.

A known shipper is a person that has an established business relationship with an indirect air carrier, an aircraft operator or an air carrier based on items such as customer records, shipping contracts, a business history and a site visit, or Dun and Bradstreet vetting. Currently, TSA allows regulated entities to use several methods to classify a shipper as known:

- Manual procedures,
- Known Shipper Database (KSDB), and
- Known Shipper Management System (KSMS).

Before TSA assumed responsibility from the Federal Aviation Administration, manual procedures were the original method for identifying known shippers. Prior to accepting cargo for transport on passenger aircraft, industry partners are responsible for conducting shipper vetting. For a shipper to be considered known, a regulated entity must ensure the existence, performance, and documentation of a customer record, along with either an established shipping contract or an established business history. The regulated entity must also conduct and document a site visit.

Customer records must contain a shipper's name, physical address, phone number, and established and verifiable business payment or credit history.

[redacted]

An established business history must consist of a previously documented business relationship between the aircraft operator and

[redacted]

The Federal Aviation Administration enhanced its manual procedures by developing the KSDB. The KSDB was an electronic repository of manually vetted shippers, which streamlined the process for regulated entities to verify the status of known shippers. Even when a participating regulated entity did not originally conduct the vetting, that entity was allowed to rely on the known shippers of other entities within the KSDB. TSA terminated operation of KSDB on October 31, 2007; however, the

[redacted]

TSA introduced KSMS for regulated entities' use in January 2007. Under KSMS, TSA conducts the vetting of domestic shippers and determines which shippers qualify for known status. Although the system is still under development, TSA is now operating KSMS and plans to mandate regulated entities' use of the system as the primary method for establishing and verifying known shippers.

TSA requires regulated entities to submit shipper data to KSMS. That data undergoes a systematic risk assessment to determine whether a shipper can be considered known. To evaluate a shipper's validity and integrity, KSMS electronically compares seven elements submitted by a regulated entity to existing business intelligence compiled by Dun & Bradstreet. KSMS applies a weighted scoring methodology by assessing the level of consistency between each corresponding element in the respective data sets. KSMS also checks shippers against a list maintained by the Department of Treasury's Office of Foreign Assets Control, which administers and enforces economic sanctions programs, primarily against countries and groups of individuals such as terrorists and narcotics traffickers. An overview of all three methods for establishing and verifying a known shipper can be found in Appendix C.

To support electronic vetting through KSMS for each potential known shipper, regulated entities are required to submit:

- Business name
- Street number
- Street name
- City
- State
- Post office box number
- Telephone number

TSA conducts inspections to ensure that regulated entities comply with known shipper requirements. TSA employs approximately 300 cargo transportation security inspectors dedicated exclusively to the oversight of air cargo security. TSA inspectors typically conduct inspections at air carriers, indirect air carriers, and all-cargo operator stations. TSA also conducts monthly special emphasis assessment tests at high-volume cargo airports, in which TSA inspectors pose as unknown shippers and attempt to ship cargo on passenger aircraft.

Results of Audit

TSA's KSP does not provide assurance that only cargo from known shippers is transported on passenger aircraft. TSA has made progress in improving the KSP by developing KSMS; however, the agency has not resolved technical problems and policy issues, which has hindered its use as the primary method for establishing and verifying known shippers.

The agency's criteria and guidance for the other two methods used to make shippers known, manual procedures and the KSDB, are unclear and subject to interpretation. This increases the risk that shippers may be improperly vetted and, therefore, unknown. TSA's oversight activities do not ensure that regulated entities are complying with KSP requirements.

Until KSMS issues are resolved, regulated entities may use any of the three KSP methods for transporting cargo on passenger aircraft. Vulnerabilities within each method increase the potential for someone to falsify or counterfeit shipping documents to become a known shipper, thereby increasing the risk to passenger aircraft security.

KSP Improvement Efforts Face Continued Challenges

TSA has made progress in modifying the KSP with the introduction of the KSMS vetting process, but the agency has been unable to fully implement the new method. TSA has not resolved ongoing technical problems and policy issues in developing and implementing KSMS, which has hindered the agency from making KSMS the primary method for establishing and verifying known shippers. Until these issues are resolved, regulated entities may use any of the three available KSP methods, which pose vulnerabilities to air cargo security.

KSMS Technical Problems

Unanticipated technical problems and performance-related issues arose during every phase of KSMS development and deployment.

After TSA launched KSMS, regulated entities experienced problems using the system. For example:

- Some regulated entities were unable to access KSMS to upload shipper lists for vetting;
- KSMS was returning vetted and appended shipper lists to the wrong party;
- KSMS was returning inaccurate shipper status determinations to some users; and
- KSMS required a lengthy amount of time to conduct start-to-finish processing of shippers, significantly delaying regulated entities' receipt of status determinations.

TSA officials and the KSMS development contractor explained that technical problems existed between the intended functional requirements and TSA's existing operating platform. The contractor was responsible for determining the functional requirements and designing a system that would work within the context of both existing and potential technologies. TSA directed the contractor to customize the database engine within the agency's existing technologies to support KSMS functionality. According to the contractor, TSA's existing technology, an Oracle database, was not designed to handle the high volume of KSMS data.

TSA's KSMS has exceeded cost expectations and is behind schedule because of these ongoing technical problems. In the majority of their weekly project status reports, the KSMS integrated project team said the overall project status was less than acceptable because of the system's technical problems and the project's inability to stay on schedule. TSA could not provide documentation to show the estimated initial costs for developing and deploying KSMS due to insufficient strategic planning for the system. We have therefore been unable to determine the extent of the delay and the associated cost overrun. However, as of July 2008, TSA had spent more than $34 million and taken more than 3 years to implement KSMS.

The KSMS project incurred delays in January 2007 because TSA could not immediately extend the contract with Dun & Bradstreet for business intelligence to support the shipper vetting process. The KSMS project manager was informed just 48 hours before the

expiration of the contract that TSA could not exercise the option year based on a new Department of Homeland Security (DHS) contracting requirement. All KSMS testing and production work stopped for nearly 3 months until the contracting issue was resolved.

TSA officials acknowledged that the agency could have prevented or alleviated some of the technical problems through better management and oversight of the KSMS project and the system's developer. TSA also indicated that KSMS performance suffered from the contractor's lack of expertise in building systems designed to perform KSMS functions, as well as insufficient contractor personnel to support the project.

KSMS Policy Issues

TSA has not resolved several KSMS policy issues. Under KSMS, a known shipper is identified by the name and physical address of the facility where the cargo is physically tendered from, not by a third-party "bill-to" address. However:

- TSA has not decided how entities can tender cargo from a location other than the shipper's physical address, such as a trade show.
- TSA has not decided how domestic known shippers with foreign business locations can tender cargo abroad for transport on passenger aircraft.

TSA is currently working to resolve these policy issues, but the agency could not estimate when they would be finished. TSA's procedures allow regulated entities to comment on the proposed changes, which the agency must consider before finalizing the policy. As a policy is changed, TSA must issue amended standard security programs for each type of entity subject to KSP requirements before declaring KSMS compliance mandatory, which may cause further delays.

Due to the ongoing technical problems and unresolved policy issues, TSA has postponed mandating the use of KSMS on several occasions. Table 1 shows TSA's repeated efforts to communicate dates for mandating KSMS as the only method for regulated entities to establish and verify known shippers.

Table 1: KSMS Delay Timetable

Date	TSA Message Regarding KSMS Implementation
January 20, 2007	After 90 calendar days, KSDB will be deactivated, making KSMS the only permissible tool for electronically verifying shippers.
March 26, 2007	Due to unforeseen system problems, TSA cannot provide a specific date when KSMS will be fully operational. In the interim, regulated entities may continue using the alternative procedures.
August 23, 2007	KSDB will be deactivated on October 31, 2007, making KSMS the only permissible tool for electronically verifying shippers.
October 12, 2007	TSA withdraws mandatory KSMS compliance as of October 31, 2007. After this date, regulated entities may use KSMS, manual procedures, or KSDB printouts to verify known shippers until April 30, 2008, or until the amended standard security programs are issued.
March 14, 2008	TSA withdraws the April 30, 2008, date and permits regulated entities to continue using any of the three methods to verify known shippers until further notice.

Until TSA mandates KSMS, regulated entities may verify known shipper status through any of the three available methods. Entities may exploit some vulnerabilities in these three systems to obtain the most favorable outcomes for their purposes. For example, KSMS may determine that a shipper matched to the Office of Foreign Asset Control list presents a security risk and therefore is ineligible to receive known status. However, when an entity has a [redacted]

KSP Manual Procedures and KSDB Do Not Ensure Passenger Aircraft Cargo Security

Manual procedures and KSDB do not provide assurances that the KSP has strengthened cargo security on passenger aircraft. TSA has not provided clear criteria and specific guidance for making a

shipper known. As a result, regulated entities may be improperly classifying shippers as known and allowing cargo from unknown shippers to be transported on passenger aircraft, posing potential risks to air cargo security.

TSA's written standard security programs do not provide enough guidance on the level of details that need to be collected and reviewed in making a shipper known through the manual procedures and KSDB. Under these methods, entities are allowed to perform minimal investigative procedures to demonstrate that these shippers are trustworthy and have adequate security measures in place to ensure the integrity of their shipments.

For example, the agency's standard security programs require entities using the manual procedures to ensure the existence of a [redacted] The established shipping contract must cover a series of shipments. However, the security programs [redacted]

TSA's standard security programs also do not sufficiently define how to establish a business history to consider a shipper known. The programs explain that an established business history consists of:

[redacted]

TSA does not specify how [redacted] must be achieved to support a business history. It implies the entity must transport the [redacted] shipments through other modes of transportation since cargo cannot be transported on passenger aircraft until a business history is established. However, this is not clear. For example, one air carrier assumed it could transport a shipper's [redacted] on its own aircraft,

but a TSA inspector cited the air carrier for improperly declaring the shipper as known.

KSP site visit verifications to substantiate a known shipper's existence are not always properly conducted. Manual procedures require regulated entities to complete a verification form while performing a site visit to a shipper's location to classify it as known, but TSA does not provide any instructions or guidance for collecting the information. With the exception of a shipper representative's signature, anyone could complete all required fields on the form without having actually visited the shipper's location to confirm its existence.

Inspection reports addressing site visit forms noted violations or confusion about the requirement to conduct site visits in conjunction with completing the form. For example:

- One airport reported that two entities allowed shippers to complete and fax back site verification forms rather than conducting on-site visits.
- At a second airport, the indirect air carrier's owner told the inspector that since he knew an individual working at the shipper's business, he considered it known and did not complete the required form.

Additionally, 14 of the TSA inspectors we interviewed said regulated entities often had concerns that the requirements for maintaining manual records were unclear and confusing.

Similar to the manual procedures, KSDB does not provide adequate assurances that a shipper is known before transporting cargo on passenger aircraft. KSDB allows a regulated entity to use

[redacted]
to verify known shippers, but the agency could not quantify the current level of KSDB usage.

By not providing specific criteria and guidance to establish and verify a known shipper, TSA provides opportunities for any shipper, including criminals or terrorists, to obtain known status without adequate verification. This shortcoming increases the opportunity for someone to falsify or counterfeit shipping documents and become a known shipper, posing vulnerabilities and possible risks to passenger aircraft security.

TSA's Inspection and Testing Activities Do Not Ensure KSP Compliance

TSA's inspection and testing activities do not provide assurances that regulated entities are complying with KSP requirements. TSA does not provide specific guidance on the inspection process, which allows varying interpretations and may lead to inaccurate results. TSA inspectors perform covert special emphasis assessment testing of regulated entities to assess compliance, but these tests are not always effective and realistic. As a result, the agency may be missing opportunities to identify areas of the KSP that could be improved to decrease vulnerabilities and strengthen air cargo security.

KSP Inspections

TSA's inspections may not accurately determine KSP compliance. Inspectors conduct these activities based on their own interpretation of the inspection guidance. The agency's national inspection manual provides limited information about the four general inspection methods that inspectors may use: surveillance, interviewing, reviewing documentation, and testing. The inspection manual does not specify to what extent each inspection method should be applied. Given such flexibilities, inspectors may favor one inspection method over the other three, which may not effectively identify KSP violations.

Some inspectors do not review enough documentation to determine KSP compliance. Inspectors use their own discretion on the types and amounts of documents to review. We reviewed the results of TSA's inspections in which inspectors determined whether regulated entities vetted known shippers according to the manual procedures. Of the 248 questions or prompts we reviewed, inspectors concluded that entities were in compliance in 112 instances. As shown in Table 2, inspectors did not [redacted] instances and verified [redacted] in [redacted] others, providing little evidence to support compliance.

Table 2: Air Waybills Reviewed to Determine Known Shipper Status

[redacted]

Additionally, inspectors frequently relied on interviews as primary support for whether regulated entities met KSP requirements. Relying on interviews may not give the inspectors enough information to identify instances of noncompliance.

[redacted]

As shown in Exhibit 1, a few exemptions allow

[redacted]

the transport of cargo from unknown shippers on passenger aircraft. We reviewed 182 inspection reports in which inspectors addressed whether indirect air carriers transported unknown shipper cargo and noted 98 instances that were "Not Applicable." These reports indicated:

- Inspectors relied primarily on interviews for 80 of the 98 instances, or 82 %. There was no additional support showing that inspectors checked documentation or observed the entities accepting cargo.
- On four inspection reports, the inspector specifically reported conclusions based on both interviews and document reviews.
- For the remaining 14 instances, we were unable to determine how the inspectors supported the conclusion that this question did not apply to the indirect air carrier.

Inspectors' frequent reliance on just one inspection method, such as an interview, to determine applicability may not identify instances of KSP violations. TSA's oversight of the KSP would be stronger when inspectors use more than one of the four general inspection methods prescribed in the inspection manual, and when they examine more documentation during their inspections.

TSA's Special Emphasis Assessment and Covert Testing of KSP Compliance

TSA's special emphasis assessment tests to determine compliance with KSP requirements are not always realistic, adequate, or reliable. According to the testing protocols, the objective of the tests is "to determine, through realistic testing," whether regulated entities are properly identifying and subsequently refusing to transport unknown shipper cargo on passenger aircraft. However, TSA's assessment testing protocols do not always consider the unique nature of the various airports' operations.

For example, a supervisory inspector reported that most of the indirect air carriers at his airport have only one or two customers. However, this official is required to perform 10 tests per month and could be recognized when testing the same entities.

Five of the inspectors interviewed believe TSA's testing protocols are not realistic for testing KSP compliance. For example:

- One inspector indicated the same inspectors tender unknown shipper packages to the air carriers monthly. After a while, the air carriers may come to recognize the inspectors.
- Another inspector said that they perform walk-up tests, even though the entities do not accept walk-up business.
- An inspector reported that indirect air carriers have their own client base and would most likely pass a test since they would direct the tester to use another carrier, such as FedEx.

Some inspectors may not be convincing as covert shippers because they fear retribution from the entities tested. The protocols require inspectors to identify themselves to aircraft operators or indirect air carriers that accept the test packages. The inspector's test could result in an employee either being removed from a job or the entity's operating privilege being revoked if someone incorrectly accepts the test package. Some inspectors expressed discomfort with using their own identification and would rather use false credentials in carrying out these duties because of potential retribution.

In August 2008, TSA's Office of Security Operations engaged the field inspectors in a working session to solicit ideas for developing future special emphasis assessment tests. Inspectors provided more than 75 suggestions, which the agency will use when developing tests for fiscal year 2009.

TSA's Office of Inspection has been planning to conduct red team covert testing of air cargo security since 2006. The agency has not performed these tests because it does not have the necessary undercover authority. TSA's Office of Chief Counsel created a legislative proposal in 2007 to resolve this authority problem, but DHS rejected the plan as not viable. TSA did not disclose the specific reasons for this rejection. In March 2008, TSA's Chief Counsel sent an informal action memo to DHS' Office of General Counsel requesting the authority; however, this request was also denied.

Unless TSA provides proper guidance and performs effective inspections and special emphasis assessment testing, the agency cannot ensure that KSP is effectively strengthening air cargo security. Also, without specific statutory authority, TSA cannot establish the covert operation it needs to perform red team tests. As a result, the agency may be missing opportunities to identify areas of the KSP that could be improved to decrease vulnerabilities and risks to air transportation.

Recommendations

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

Recommendation #1: Resolve all remaining Known Shipper Management System technical problems and policy issues so that the agency can target and achieve a specific date for mandating regulated entities compliance with the new method.

Recommendation #2: Document and share with all Department of Homeland Security personnel involved in procurement actions, the experience and lessons learned from the contracting and development of the Known Shipper Management System for use in improving future agency program enhancements.

Recommendation #3: Enhance the criteria and guidance used in the manual process for making a shipper known to provide greater assurance that shippers are legitimate and pose a minimal threat to aviation security. Specifically, the agency should provide better direction on the frequency and efforts required to validate the existence, performance, and documentation of each known shipper.

Recommendation #4: Provide more specific guidance to inspectors conducting reviews of Known Shipper Program compliance, including the level of review and effort necessary to verify known shipper status, the amount of documentation and air waybills to examine, and the appropriate balance in the application of the four basic inspection methods.

Recommendation #5: Revise special emphasis assessment testing protocols to reflect more realistic scenarios. Specifically, the agency should revise the protocols based on the many suggestions

solicited from field inspectors so the testing will be more reliable to gauge compliance.

Recommendation #6: Continue to work with the Office of General Counsel to obtain undercover authority that would allow the agency to perform red team covert testing of Known Shipper Program compliance and air cargo security.

Management Comments and OIG Analysis

TSA generally concurred with the recommendations in the report. The agency will use the findings and recommendations to continue to improve the KSP.

TSA's response indicated that the KSP is an important layer in securing the air cargo supply chain, but is by no means the only mechanism used to strengthen air cargo security. Rather, the KSP provides one measure of security by establishing a valid business relationship between shippers and regulated entities that accept cargo for transport by air. Other critical layers of TSA's Air Cargo Security Strategy include security threat assessments, cargo screening and compliance inspections.

TSA also noted that the agency has recently made improvements to its Air Cargo Security Enforcement Program. For example, TSA's Fiscal Year 2008 Regulatory Activities Plan directed Transportation Security Inspectors to conduct at least two critical inspections per year at air carriers and indirect air carriers to determine whether an entity is in compliance with known shipper requirements. At least once a month at various locations, TSA conducts Cargo Strikes, which are week-long regulatory compliance "blitzes" of a target airport's regulated air cargo community. In fiscal year 2008, TSA conducted nearly 4,000 covert tests of both foreign and domestic air carriers and indirect air carriers in regard to known shipper security requirements.

Management Comments to Recommendation 1:

TSA Concurs. TSA has aggressively proceeded with several modifications to KSMS to correct issues which kept the system from operating at a level which could support mandatory use. These modifications were developed by TSA and are in the final stages of

testing. Once in production, an evaluation period will be necessary to validate the performance and quality standards prior to issuing a mandatory requirement. TSA intends to make KSMS mandatory when all technical problems and policy issues are fully resolved.

OIG Analysis: We recognize TSA's efforts to correct the KSMS deficiencies by making modifications to the automated system which could support mandatory use. This recommendation is resolved but will remain open until TSA requires mandatory use of KSMS.

Management Comments to Recommendation 2:

TSA concurs, in part. TSA concurs that the agency will benefit from a structured review of the program management challenges presented by KSMS and from the identification of lessons learned. TSA does not agree that sharing lessons learned across the Department would be beneficial. Many of TSA's challenges with the program can be attributed to the fact that KSDB was deemed to be a short-term fix that was not meant to last more than 6 months. However, because of more pressing agency priorities, KSDB lasted 5 years.

OIG Analysis: TSA's response acknowledges that the agency could have prevented or alleviated some of the technical problems through better management and oversight of the KSMS project and the system's developer. TSA also indicated that KSMS performance suffered from the contractor's lack of expertise in building systems designed to perform KSMS functions, as well as insufficient contractor personnel to support the project. We believe these experiences would be a valuable lesson for other DHS personnel involved in procurement actions. Accordingly, this recommendation is unresolved and will remain open.

Management Comments to Recommendation 3

TSA Concurs, in part. TSA's response did not clearly identify why the agency partially concurred. TSA is currently revising the known shipper portions of the standard security programs to provide more specific details to the regulated parties regarding the criteria to make a shipper known using the manual approach. The standard security programs were scheduled for publication in December 2008. TSA noted that some regulated parties have chosen not to fully comply with procedures outlined in the standard security programs for making a shipper known through the manual method. As such, TSA will continue to aggressively pursue enforcement action against these parties when violations are discovered.

OIG Analysis: The issuance of the revised standard security programs should provide greater assurance that shippers are legitimate. This recommendation is resolved but will remain open until we have the opportunity to review the security programs.

Management Comments to Recommendation 4

TSA Concurs. TSA has already started several different initiatives that effectively provide Transportation Security Inspectors more specific guidance for conducting reviews of KSP compliance. Some examples include an enhanced training curriculum, revising the National Inspection Manual, and more in-depth reviews of the regulated entities involving known shipper requirements.

Because of the large number of business models in use, the regulated entities must have flexibility to prove compliance with KSP requirements. Transportation Security Inspectors must have flexibility to use different methods of inspection to determine compliance with these requirements. Rather than prescribe exactly how many documents to review or how many personnel to interview, TSA ensures Transportation Security Inspectors have flexibility by training them in inspection and investigation techniques and then empowering them to use inspector discretion to determine compliance.

OIG Analysis: The enhanced training, guidance, and more comprehensive inspections should provide better testing of the known shipper requirements. This recommendation is resolved but will remain open until we have the opportunity to review the enhanced inspector training curriculum and National Inspection Manual revisions.

Management Comments to Recommendation 5

TSA Concurs. TSA has begun revising its special emphasis assessment testing protocols. The agency is modifying the special emphasis assessment testing protocols, based on nearly 100 unique suggestions from field Transportation Security Inspectors who attended a National Transportation Security Inspector Cargo Conference in August 2008. TSA expects to implement the new protocols in the second quarter of fiscal year 2009.

OIG Analysis: This recommendation is resolved but will remain open until we have the opportunity to review documentation supporting that the new special emphases testing protocols have been implemented.

Management Comments to Recommendation 6

TSA Concurs. TSA's Office of Chief Counsel has submitted to DHS Office of General Counsel a revised legislative proposal and is working with the OGC to complete an Administration review.

OIG Analysis: This recommendation is closed.

The objective of our audit was to determine whether TSA's policies and procedures for the Known Shipper Program provide assurances that cargo is secure for transport on passenger aircraft. We also determined whether TSA's inspections of regulated entities provide assurances that those entities are complying with KSP requirements.

We obtained and reviewed applicable federal laws and regulations, TSA's standard security programs, security alerts, cargo information bulletins, the National Inspection Manual, the Air Cargo Strategic Plan, and other related documents.

We interviewed TSA personnel from the Offices of Transportation Sector Network Management, Security Operations, Inspections, and Chief Counsel. We also interviewed representatives from TSA's Information Technology Division, Solution Delivery Branch, and contractors responsible for the development and support of the KSMS.

We visited and interviewed inspectors at three Category X airports. At two of the three, we observed TSA personnel performing inspections at aircraft operators, all-cargo operators, and indirect air carrier facilities.

We also conducted a review and analysis of ten of the 18 Category X airports that transported the most freight during fiscal year 2007. They were:

- John F. Kennedy International;
- Los Angeles International;
- Chicago O'Hare International;
- Hartsfield-Jackson Atlanta International;
- Miami International;
- San Francisco International;
- Washington-Dulles International;
- Honolulu International;
- Newark-Liberty International Airport; and
- Dallas/Fort Worth International.

We obtained summary TSA reports documenting the total number and type of inspections each airport performed on the known shipper requirements completed at each location between October 1, 2006, and March 31, 2008. We also obtained several reports

summarizing the numbers and types of violations inspectors disclosed during their inspections. We judgmentally selected and analyzed 381 inspection reports to determine the quality of TSA's inspection efforts. We developed a questionnaire and interviewed 22 TSA inspectors at these airports.

We conducted this performance audit according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted fieldwork between April 2008 and August 2008 under the authority of the *Inspector General Act of 1978*, as amended.

Appendix B
Management Comments to the Draft Report

~~SENSITIVE SECURITY INFORMATION~~

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

JAN 1 4 2009

Transportation Security Administration

INFORMATION

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

FROM: Kip Hawley
Assistant Secretary

SUBJECT: Transportation Security Administration (TSA) Response to the DHS Office of the Inspector General's Draft Report: *Transportation Security Administration's Known Shipper Program*, October 2008

Purpose

This memorandum constitutes TSA's response to the DHS Office of Inspector General's (OIG) Draft Report, *Transportation Security Administration's Known Shipper Program*. TSA appreciates OIG's effort in this audit and will use the findings and recommendations to continue to improve the Known Shipper Program (KSP).

Background

OIG conducted its review between January and October 2008. The audit objectives were to determine whether the policies and procedures of the KSP provide assurances that cargo is secure for transport on passenger aircraft, and that TSA's compliance inspections provide assurances that KSP policies and procedures are followed.

OIG found that while TSA has made progress improving some aspects of the KSP, the agency's criteria and guidance for evaluating whether a shipper meets Known Shipper requirements are unclear and subject to interpretation, and inspection activities do not provide assurances that regulated entities are complying with the KSP's vetting requirements.

Discussion

TSA appreciates OIG's work in its evaluation of the KSP, one of many layers protecting the transportation of air cargo on passenger aircraft. As discussed below, the passenger air cargo network is protected by a multi-layered security system actively deploying an

advanced screening system. Also, TSA's air cargo security inspection program has implemented major enhancements to air cargo security.

The Known Shipper Program is One of Multiple Security Layers for Air Cargo

A known shipper is a person or company that can demonstrate an established business relationship with a freight forwarder. This relationship is verified through items such as customer records, shipping contracts, and a business history. The KSP is an important layer in securing the air cargo supply chain but is by no means the only mechanism used to strengthen air cargo security. Rather, the KSP provides one measure of security by establishing a valid business relationship between shippers and regulated entities that accept cargo for air transport.

Other critical layers of TSA's Air Cargo Security Strategy include:

1) Vetting to ensure that entities and people meet security standards. Vetting includes requiring anyone with access to air cargo to undergo a security threat assessment and ensuring that a prospective indirect air carrier (IAC) is a legitimate business before granting them an IAC certificate.

2) Screening cargo using approved screening methods and technologies. Currently, air carriers are required to screen a certain percentage of air cargo on passenger aircraft for explosives using screening methods such as physical search, X-ray, and Explosives Trace Detection. TSA conducts 100 percent screening for certain categories of cargo deemed to be high risk and destined for passenger aircraft [redacted] Air cargo destined for all-cargo aircraft is screened by carriers for stowaways.

An important layer of TSA's screening regime is its canine screening force. TSA currently supports about 468 local law enforcement led canine teams at 79 domestic airports. These teams spend approximately 25 percent of their time in the cargo environment. Furthermore, TSA is deploying 85 TSA-led teams focused solely on screening air cargo and associated facilities at high-volume airports within the United States. Beginning in 2005, TSA increased funding for canine screening using monies previously tagged for the development of the Known Shipper Management System (KSMS), which enabled TSA to allocate more resources to canine which are directly engaged in the screening of air cargo. Allocating additional resources to this layer of security has provided TSA with better flexibility in mitigating risk and targeting ever-changing threats.

TSA also recently initiated several new screening programs to increase the current level of air cargo security.

- ***The Narrow-body Screening Amendment.*** By requiring 100 percent screening of cargo transported on all narrow- bodied passenger aircraft, TSA has drastically increased air cargo security by protecting the vast majority of passengers on passenger aircraft. This requirement was implemented by a regulatory program amendment which took effect in October 2008.

- ***The Certified Cargo Screening Program (CCSP).*** The CCSP is a new initiative to assist the air cargo industry in meeting the mandates of the *Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act)* which requires 50 and 100 percent screening for cargo being flown on passenger aircraft by February 2009 and August 2010, respectively. Once fully enacted, CCSP will ease the burden on air carriers by expanding the industry's screening capacity, allowing security minded companies such as IACs, manufacturing facilities, third party logistic companies, and shippers to share with air carriers the regulatory screening burden.

- ***The Indirect Air Carrier Screening Technology Pilot.*** TSA has implemented a screening technology pilot with certain high-volume IACs participating in the CCSP. The pilot creates screening capacity at high volume IACs, measures the effectiveness of select screening technologies on various commodity classes, and evaluates chain-of-custody procedures for screened cargo as it moves from the IAC to the air carrier.

3) Assessments of regulated entities' compliance with security requirements. TSA also employs over 450 air cargo inspectors to ensure that IACs, air carriers and their authorized representatives are in compliance with TSA air cargo security regulations.

TSA has Implemented Significant Improvements to its Air Cargo Security Enforcement Program

In its draft report, OIG accurately assesses many of the KSP's challenges. It must be noted, however, that the report does not fully reflect recent improvements made to the program. For example:

- TSA operates a robust inspection and compliance program to ensure the integrity and security of the KSP. TSA's FY08 Regulatory Activities Plan (RAP) directed Transportation Security Inspectors (TSIs) to conduct at least two critical inspections per year at air carriers and IACs to determine their compliance with known shipper requirements. It is worth noting that the National Inspection Manual (NIM) identifies a known shipper violation as one that merits the maximum civil penalty.

- TSA conducts Cargo Strikes, which are week-long regulatory compliance "blitzes" of a target airport's regulated air cargo community. These concentrated events enhance TSA's ability to assess whether regulated entities in a given community are adhering to known shipper and other cargo security requirements. Cargo Strikes use TSIs from target and other airports to promote nation-wide consistency and are conducted at least once per month at various locations.

- TSIs are required to test foreign and domestic air carriers and IACs for compliance with known shipper security requirements. During these tests, a TSA employee will covertly pose as an unknown shipper in an attempt to ship a piece of cargo on a passenger aircraft. In FY08, TSA required 2,400 covert tests at airports across the Nation. TSIs exceeded this requirement by conducting nearly 4,000 tests. Associated enforcement actions have been taken with respect to these tests.

- Since 2003, TSA has revoked the TSA security program approval of 14 IACs, preventing these businesses from shipping cargo on passenger aircraft. Revocation constitutes the most serious enforcement action TSA can take. The vast majority of these revocations (10) stem directly from investigations into violations of the known shipper requirements. One IAC was indicted, and its principal owner served a prison sentence for criminal activities involving falsification of known shipper records.

Conclusion

TSA appreciates OIG's work on this audit and will take the recommendations under advisement. As we have indicated, the KSP constitutes one of many layers in the air cargo security system, which is expanding its focus to ensure that all cargo carried on passenger aircraft is screened for explosives in a manner that does not impede commerce.

TSA's response to OIG's recommendations is attached.

~~SENSITIVE SECURITY INFORMATION~~

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

***TSA's Known Shipper Program*, October 2008**

Recommendation 1: Resolve all remaining Known Shipper Management System technical problems and policy issues so that the agency can target and achieve a specific date for mandating regulated entities compliance with the new method.

TSA Concurs. TSA has proceeded aggressively with several modifications to the automated system to correct issues which kept the system from operating at a level which could support mandatory use. TSA developed these modifications which are in the final stages of testing. Once the system is in production, an evaluation period will be necessary to validate the system's performance and quality before TSA issues a mandatory requirement. TSA intends to make the Known Shipper Management System (KSMS) mandatory when all technical problems and policy issues are fully resolved.

Recommendation 2: Document and share with all Department of Homeland Security personnel involved in procurement actions, the experience and lessons learned from the contracting and development of the Known Shipper Management System for use in improving future agency program enhancements.

TSA Concurs, in part. TSA concurs that it will benefit from a structured review of the program management challenges presented by KSMS and from identifying lessons learned. TSA does not agree that sharing lessons learned across the Department would be beneficial. Many of TSA's challenges with the program can be attributed the fact that the Known Shipper Database (KSDB) was deemed to be a short-term fix that was not meant to last more than 6 months. However, because of more pressing agency priorities, KSDB lasted 5 years.

Recommendation 3: Enhance the criteria and guidance used in the manual process for making a shipper known to provide greater assurance that shippers are legitimate and pose a minimal threat to aviation security. Specifically, the agency should provide better direction on the frequency and efforts required to validate the existence, performance, and documentation of each known shipper.

TSA Concurs, in part. TSA is currently revising the known shipper portions of the standard security programs to give regulated parties more detail regarding the criteria for making a shipper known via the manual approach. The standard security programs are scheduled for publication in December 2008. Notwithstanding these revisions, it must be recognized that some regulated parties have chosen not to fully comply with procedures

outlined in the standard security programs for making a shipper known via the manual method. TSA has and will continue to aggressively pursue enforcement action against these parties when violations are discovered.

Recommendation 4: Provide more specific guidance to inspectors conducting reviews of Known Shipper Program compliance, including the level of review and effort necessary to verify known shipper status, the amount of documentation and air waybills to examine, and the appropriate balance in the application of the four basic inspection methods.

TSA Concurs. Because of the large number of business models in use, the regulated entities must have flexibility to prove compliance with Known Shipper Program (KSP) requirements. Transportation Security Inspectors (TSIs) must have flexibility to use different methods of inspection, including Surveillance, Interview, Document Review, and Testing (SIDoT), to determine compliance with these requirements. Rather than prescribe exactly how many documents to review or how many personnel to interview, TSA ensures TSIs have flexibility by training them in inspection and investigation techniques and then empowering them to use discretion to determine compliance.

Nonetheless, TSA has started several initiatives that give TSIs more specific guidance for reviewing KSP compliance. Some examples include:

- **Recurrent training.** In FY08, TSA instituted recurrent training for TSIs who completed the core class over 3 years ago. This training refreshes the inspection and investigation skills of the workforce and gives them updated information.
- **Enhanced training.** TSA is enhancing the core TSI training curriculum to better instruct new TSIs in the four basic inspection methods. TSA expects the improved curriculum to be ready by the end of FY09.
- **Specially trained instructors.** TSA is using specially trained TSI instructors who are operational field TSIs to teach the cargo portions of the core class. This ensures that TSIs benefit from field knowledge and experience.
- **Enhanced On the Job Training (OJT).** TSIs spend two weeks with specially trained TSI instructors and shadow them as they conduct all facets of the inspection and investigation process. This enhanced OJT exposes TSIs to environments other than their home airport and focuses on the SIDoT methodology.
- **Online Training.** In October 2008, TSA established a series of quarterly training online seminars for cargo TSIs. This training helps update and enhance the workforce's inspection and investigation skills.

- **Inspector Handbook**. The Nation Inspection Manual (NIM) is currently under revision and will be reissued as the Inspector Handbook. Assistant Federal Security Directors-Inspection (AFSDs-I) and field TSIs are driving the revisions to ensure the field perspective is included. Among other elements, the revised handbook will feature best practices that inspectors might employ in air cargo security and KSP inspections. The new handbook is expected to be completed in FY09.

As for guidance on the level of review, the FY08 Regulatory Activities Plan (RAP) required at least one critical inspection per passenger air carrier and indirect air carrier (IAC) during a six month period. The KSP is included during a critical inspection. The FY09 RAP requires more in-depth reviews of all regulated entities, to include air carriers and IACs. These reviews are designated "comprehensive" and include Known Shipper requirements. Additionally, the FY09 RAP also requires supplemental inspections which focus on specific areas of regulation.

Moving forward, TSA will continue to explore and identify appropriate opportunities for additional KSP guidance. For example, in FY09, TSA will continue developing new guidance and testing protocols focused on high risk areas of air cargo security. This initiative, along with an overall expansion of compliance testing, will increase the number of tests conducted.

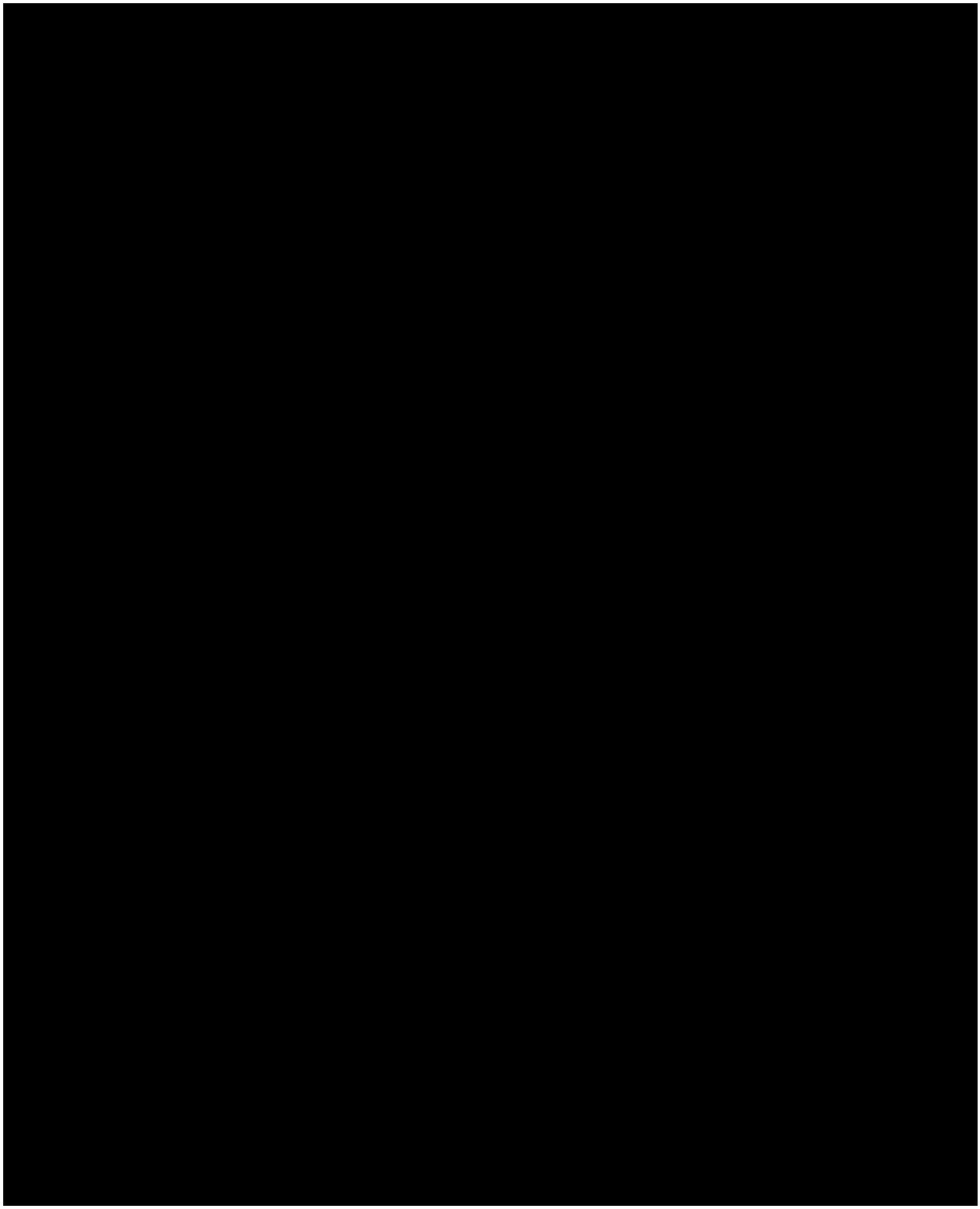
Recommendation 5: Revise special emphasis assessment testing protocols to reflect more realistic scenarios. Specifically, the agency should revise the protocols based on the many suggestions solicited from field inspectors so the testing will be more reliable to gauge compliance.

TSA Concurs. New special emphasis assessment (SEA) testing protocols, based on nearly 100 unique suggestions from field TSIs who attended the recent National TSI Cargo Conference (August 2008), are expected to be implemented in the second quarter of FY09.

Recommendation 6: Continue to work with the Office of General Counsel to obtain undercover authority that would allow the agency to perform red team covert testing of Known Shipper Program compliance and air cargo security.

TSA Concurs. TSA's Office of Chief Counsel has submitted to DHS Office of General Counsel (OGC) a revised legislative proposal and is working with the OGC to complete Administration review.

[redacted]



Appendix D
Major Contributors to this Report

Patrick O'Malley, Director
Dennis Deely, Audit Manager
Robert Ferrara, Auditor-In-Charge
Gary Alvino, Program Analyst
Tia Jackson, Program Analyst
James Bess, Referencer

Department of Homeland Security

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

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4199, 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.