



# Department of Homeland Security Office of Inspector General

## Security of Air Cargo During Ground Transportation

(Redacted)



Office of Inspector General

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



Homeland  
Security


NOV - 5 2009

### Preface

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

This report addresses the strengths and weaknesses of the Transportation Security Administration's efforts to secure air cargo during ground transportation and handling before it is loaded onto planes for air shipment. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. 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

---

Executive Summary .....	1
Background.....	2
Results of Audit .....	5
Air Cargo Security Vulnerabilities .....	5
Air Cargo Security Inspections.....	10
Recommendations.....	14
Management Comments and OIG Analysis .....	16

## Appendixes

Appendix A: Purpose, Scope, and Methodology.....	21
Appendix B: Management Comments to the Draft Report.....	23
Appendix C: Process for Ground Transportation of Air Cargo .....	31
Appendix D: Security Threat Assessment Requirements.....	32
Appendix E: Major Contributors to This Report .....	33
Appendix F: Report Distribution .....	34

## Abbreviations

DHS	Department of Homeland Security
FY	Fiscal year
OIG	Office of Inspector General
PARIS	Performance and Results Information System
TSA	Transportation Security Administration

# OIG

---

*Department of Homeland Security  
Office of Inspector General*

## **Executive Summary**

This report addresses the effectiveness of the Transportation Security Administration's efforts to secure air cargo while it is handled or transported on the ground, prior to being shipped on passenger aircraft.

The Transportation Security Administration could improve its efforts to secure air cargo during ground handling and transportation. We determined that personnel were sometimes accessing, handling, or transporting air cargo without the required background checks or training. For example, of the drivers we tested were handling or transporting air cargo without the required background checks. We also reviewed drivers' records and identified that 23% did not satisfy the required training and testing requirements.

The agency's inspection process has not been effective in ensuring that requirements for securing air cargo during ground transportation are understood or followed. The inspection process has focused on quantity rather than outcomes and ensuring corrective actions. Automated tools to assist inspectors in analyzing results and focusing their oversight efforts on high-risk areas in air cargo security were not adequate. As a result, air cargo is vulnerable to the introduction of explosives and other destructive items before it is loaded onto planes, potentially creating risks for the traveling public.

We are making six recommendations to the Transportation Security Administration that, when implemented, would strengthen the security of air cargo during ground transportation. The agency concurred with five recommendations and partially concurred with one recommendation.

---

## Background

The Transportation Security Administration (TSA) is responsible for overseeing aviation security and ensuring the safety of the air traveling public. This responsibility includes screening, inspecting, and ensuring the security of freight that is to be transported on aircraft. TSA estimates that 12 million pounds of cargo is loaded onto passenger-carrying planes every day. Air cargo includes items such as electronic equipment, automobile parts, clothing, medical supplies, fresh produce, and human remains.

Air cargo begins with a shipper who tenders one or more packages to an indirect air carrier, also known as a freight forwarder. Among other things, indirect air carriers consolidate cargo from many shippers and deliver it to air carriers. The indirect air carrier's trucking employees, or authorized representatives<sup>1</sup> transport the cargo in locked, sealed, or monitored trucks to the airlines for air shipment. Appendix C provides more details regarding the air cargo ground transportation process.

TSA regulates air carriers, indirect air carriers, and all-cargo carriers through requirements in the agency's security programs. These include the Aircraft Operator Standard Security Program, Model Security Program, Indirect Air Carrier Standard Security Program, and Full All-Cargo Standard Security Program. The regulated entities must ensure that all of their authorized representatives comply with the security programs. TSA's air cargo security programs are designed to protect persons and property traveling by air against the introduction of any unauthorized person, explosive, incendiary, or destructive substance or item into cargo onboard an aircraft, while not impeding the flow of commerce.

---

<sup>1</sup> An authorized representative, such as an agent, contractor, or subcontractor, is an individual who is not an employee of a regulated entity but is authorized to act on the behalf of the entity to perform measures required by the security programs.

---

To help ensure compliance with the air cargo security requirements, TSA relies on the oversight carried out by approximately 435 cargo inspectors located throughout the United States. Under each security program, inspectors review a number of required items as they apply to each regulated entity. The cargo inspectors perform the following types of inspections:

- **Comprehensive** inspections are in-depth analyses of an entity's security operations that address every regulatory requirement, and are conducted at least once per year.
- **Supplemental** inspections provide emphasis for items that require more frequent attention. For example, these inspections are used to follow up on findings discovered during previous inspections, or are based on national or local intelligence or trends. Supplemental inspections are conducted on an as-needed basis.
- **Special emphasis** inspections focus on a particular issue or area, such as access control. Directed by TSA headquarters, these inspections are narrowly focused on a regulatory requirement and may be time sensitive.

The inspectors also provide the opportunity for regulated entities to ask questions and seek clarification regarding policies and procedures. According to TSA's Fiscal Year (FY) 2009 Regulatory Activities Plan, this outreach is a means to enhance partnership with industry, stakeholders, and with other government agencies. Inspectors should conduct outreach in their area of responsibility on an ongoing basis to provide guidance regarding transportation security to regulated entities. The type of outreach conducted may be related to guidance regarding security measures, security meetings, special events, exercises, TSA-approved training, and other transportation security-related efforts.

The inspectors document the results of their inspections in TSA's Performance and Results Information System (PARIS). PARIS is a tool for managing and analyzing data, monitoring compliance, measuring performance, and researching allegations

---

of noncompliance with statutory or regulatory air cargo security requirements.

In 2007, the Congressional Research Service reported that the large estimated number of cargo thefts and other cargo crimes indicated potential weaknesses in air cargo security.<sup>2</sup> The Congressional Research Service reported that cargo crime is committed either by or with the assistance of cargo workers, and therefore, anticipated that increased security measures, such as conducting more stringent or more frequent background checks of cargo handlers and transporters and enhanced physical security of cargo operations areas would likely improve the capability to detect criminal activity in air cargo operations.

In June 2008, TSA's Office of Intelligence reported that transportation was the most threatened sector for terrorist activity, and aviation was a high-priority target. TSA noted that terrorists would likely continue to seek out vulnerabilities and bypass security measures for cargo shipments on passenger aircraft. Like the Congressional Research Service, TSA identified insiders - individuals with authorized access to sensitive areas, equipment, or information - as one of the greatest threats to aviation.

To strengthen air cargo security, TSA recently introduced the voluntary Certified Cargo Screening Program. This program relies on vetted, validated, and certified cargo screening facilities to screen cargo prior to tendering it for transport on passenger aircraft. The recommendations of the 9/11 Commission Act of 2007 mandates the Department of Homeland Security (DHS) to establish a system to screen 100 percent of cargo transported on passenger aircraft by August 2010. Although the Certified Cargo Screening Program will relieve the air carriers from having to screen all of the cargo to meet this mandate, air carriers must ensure that all cargo has been screened prior to flight. One of the new program's key tasks is controlling and tracking the screened air cargo's chain of custody, which includes a network of

---

<sup>2</sup> Congressional Research Service Report for Congress "Air Cargo Security," Updated July 30, 2007.

---

regulated entities and their third party carriers responsible for ensuring the safety of air cargo.

## Results of Audit

TSA could improve its efforts to ensure air cargo is secure during ground handling and transportation. We determined that personnel were accessing, handling, or transporting air cargo without the required background checks or training. For example, we

- gained access to air cargo at [redacted] of the facilities visited,
- identified [redacted] of the drivers tested were handling or transporting air cargo without required background checks, and
- identified 23% of the drivers tested did not satisfy the required training and testing requirements.

Despite identifying and reporting similar vulnerabilities, TSA's inspection process has not effectively ensured improved compliance and awareness of TSA's requirements. The process has focused on quantity rather than outcomes and ensuring corrective actions. Automated tools to assist inspectors in analyzing results and focusing their oversight efforts on high-risk areas in air cargo security were not adequate. As a result, air cargo is vulnerable to the introduction of explosives, incendiaries, and other destructive items before it is loaded onto planes, potentially creating risks for the traveling public.

## Air Cargo Security Vulnerabilities

Air carrier employees or their representatives were accessing, handling, or transporting air cargo without the required background checks or training. During the first three quarters of FY 2008, TSA conducted 6,767 cargo security inspections, of which 2,031 inspections (30%) identified 2,640 air cargo security violations including:

- 
- 254 violations related to access controls,
  - 731 violations related to security threat assessments, and
  - 1,655 violations of security training and testing requirements.

Our audit also identified security violations in these areas.

### **Access Controls**

TSA's security programs require regulated entities to control access to areas where air cargo is stored. In addition to physical security, the regulated entities must have procedures in place for challenging all unknown persons who enter secure cargo areas. However, TSA inspection reports identified 254 instances of access control violations, and we gained unescorted access to air cargo at \_\_\_\_\_ of the regulated facilities we visited. For example,

- At an indirect air carrier facility, we gained access to air cargo through an unmanned door with a defective lock. Although an alarm sounded, no warehouse personnel responded to challenge our access. We had access to multiple storage rooms, including one which contained cargo that had been screened and was being shipped that evening on a passenger aircraft.
- At another air carrier facility, we gained access to an air cargo storage room through an unlocked door. At the same facility, we encountered a number of individuals but were never challenged. One employee opened a second door allowing us access to the tarmac and runway. A number of other individuals allowed us to walk around without being challenged.

Without regular vigilance, practice, and enforcement of access controls, TSA and the regulated entities provide opportunities for individuals to introduce explosives, incendiaries, and other

---

destructive items into air cargo, potentially creating risks for the traveling public.

### **Security Threat Assessments**

TSA's security programs require that regulated entities perform security threat assessments (background checks) on all individuals working for or on behalf of the regulated entities who have unescorted access to air cargo. The background checks are to be completed before the individuals begin handling or transporting air cargo. In lieu of the security threat assessment, TSA regulations provide for accepting documents which demonstrate that the individual has undergone a background check. These equivalent documents include a commercial driver's license with a hazardous material endorsement, a Transportation Worker Identification Credential,<sup>3</sup> or a Free and Secure Trade<sup>4</sup> card. Regulated entities must provide supporting documentation to verify that personnel have received the required security threat assessment or that the individual has an approved equivalent. Appendix D provides more information regarding TSA's security threat assessment requirements.

TSA inspection reports identified 731 instances where regulated entities either did not conduct or provide evidence that employees or authorized representatives had undergone background checks. We identified \_\_\_\_\_ drivers sampled who were handling and transporting air cargo without meeting TSA's security threat assessment requirement. For example,

- A truck driver displayed an employee identification card that had his photo, but a coworker's name. After

---

<sup>3</sup>The Transportation Worker Identification Credential is a common identification credential that uses smart card technology to link an individual to a specific credential.

<sup>4</sup> The Free and Secure Trade program is a joint program between the Canada Border Services Agency and the United States Customs and Border Protection. The program offers preauthorized importers, carriers and drivers expedited clearance for eligible goods.

---

following up on his identity, we determined the truck driver had never applied for a security threat assessment and had been handling cargo for almost a year and half.

- Five delivery drivers for one indirect air carrier were handling and transporting air cargo without security threat assessments.
- Three drivers from a regulated entity's authorized representative did not have security threat assessments.

TSA's security programs and the regulations do not provide assurance that entities accurately verify the identification of personnel seeking a security threat assessment. TSA's security programs and 49 CFR 1540.203 require regulated entities to verify the identity of each applicant by reviewing two forms of identification, one of which must be a government-issued picture identification, or other means approved by TSA. In addition, the regulations do not require that regulated entities maintain copies or list the documents reviewed to ensure each applicant's identity was properly authenticated. Therefore, TSA can not be sure proper personnel are handling or transporting air cargo.

Additionally, the security threat assessment application does not require a Social Security number. Instead, this is an optional field on the application. While submission of the Social Security number is voluntary, 49 CFR 1540.203 indicates that the failure to provide the information may delay or prevent completion of the threat assessment process. The verification of a Social Security number with the applicant's identification would reduce the risk of false identification.

TSA officials indicated that applicants are not vetted against [REDACTED] because the regulations do not require this. Instead, the applicants' information is vetted against terrorist-based lists, such as the No Fly, Selectee, and Terrorist Screening Database, also known as the Terrorist Watch List.

[REDACTED], TSA

---

allows questionable individuals opportunities to obtain approved clearances for handling or transporting air cargo. As a result, individuals could introduce explosives and other destructive items into cargo, posing a risk to the industry and traveling public.

### **Cargo Security Training**

TSA's security programs require that all personnel working for or on behalf of a regulated entity who have unescorted access to air cargo complete initial and recurrent security training, and pass an exam with a score of 85% or better. Regulated entities' employees or authorized representatives either did not take the initial or annual recurrent security training and pass the required examinations or could not provide evidence of meeting these requirements.

TSA inspection reports identified 1,655 violations related to the security training and testing requirements. We determined that 24 of 104 (23%) truck drivers had not completed or could not provide evidence to satisfy this requirement. For example, drivers at one indirect air carrier had taken only the initial training and testing. The security coordinator for another indirect air carrier did not test his employees on the annual recurrent training.

The security training and testing violations occurred in part because regulated entities were unaware of the requirements, including the requirement to have supporting documentation available upon TSA's request. A security manager at one location explained that he was unaware of the annual recurrent training requirement. The indirect air carrier's security coordinator received a letter from TSA with revisions to the security program requirements; however, he thought the change applied to the annual recurrent training requirements. According to some TSA inspectors, although inspectors are expected to conduct outreach in their area of responsibility on an ongoing basis to provide guidance regarding transportation security, they

---

have limited time for in-depth discussions pertaining to training or any other security measures.

By not ensuring that regulated entities' employees or authorized representatives take or pass the required security training, TSA limits personnel from effectively safeguarding air cargo against the introduction of explosives and other destructive items into cargo, posing a risk to the industry and traveling public.

## **Air Cargo Security Inspections**

The air cargo security violations we observed during our visits and reported by TSA inspectors persist because TSA's inspection process has not been effective in ensuring compliance and awareness of air cargo security requirements. Based on our review of summary inspection reports for FYs 2007 and 2008 and observations made during our site visits, there are repeat patterns of violations that TSA has been unable to resolve. TSA does not have a robust inspection process that focuses on high risk areas. Automated tools to assist inspectors in identifying, documenting, and focusing their oversight efforts on high risk areas in air cargo security are not adequately used. As a result, TSA misses opportunities to strengthen aviation security through its inspection process and reduce the risk to air cargo before it is loaded onto planes.

### **TSA's Inspection Process**

TSA's FY 2009 Regulatory Activities Plan does not emphasize high-risk areas. Instead, the plan requires that each regulated entity receive a comprehensive inspection at least once per year, and indicates that each nonsupervisory inspector must complete a minimum of 29 inspections per quarter. This number may include supplemental follow-up inspections for entities that are not in compliance. A cargo inspector who satisfies his or her annual inspection quota is expected to perform additional inspections under the guidance of local airport leadership.

The Regulatory Activities Plan does not allow inspectors to allocate sufficient time to visit entities that do not comply with

---

security procedures. One inspector said that too much emphasis is placed on accomplishing the quantity of inspections each quarter, causing the quality of inspections to suffer. Another inspector indicated that inspectors' time and efforts could be better used by focusing more on the problem entities and less on those that are in compliance. The inspector said that comprehensive reviews are almost 30 pages long and very time-consuming to complete, even for entities that are in compliance.

The Regulatory Activities Plan does not consider the additional time required for inspectors to visit regulated entities and address questions regarding the security requirements. During our site visits to several entities, personnel expressed confusion about some of the security requirements and requested the opportunity to ask the inspectors questions on a range of topics. Because of the aggressive inspection schedule and quota, as well as the time required to document each inspection, inspectors usually visit a regulated entity only once a year, unless follow-up is needed as a result of the first inspection.

#### **Analytical Tools Not Effectively Used for Targeting High Risk Areas**

Another factor limiting the effectiveness of TSA's inspection activities is that the agency does not effectively use analytical tools for targeting inspections to high-risk areas. While PARIS has been improved in the past several years, some inspectors are reluctant to rely on the system because of its limited reporting capabilities and other functional problems. Some inspectors said PARIS is slow, lacks necessary functionality, and often crashes. For example, some inspectors indicated that PARIS could not supply information on past inspections for entities. Therefore, they had to obtain the information from the inspector who conducted the last review to determine what areas required more attention. In addition, inspectors were unable to obtain the entities' address in PARIS and had to rely on other sources instead.

---

The PARIS database cannot automatically analyze data and report trends. Therefore, trend analysis requires the user to extract, sort, and filter the data using programs such as Excel or Access and post the information on TSA's SharePoint for airports to use. According to TSA headquarter officials, airports may use analytical reports developed from PARIS data; however, not all are doing so. A majority of the supervisory inspectors at the airports we reviewed indicated that they did not rely on PARIS trends and analysis when planning inspections. Some airports develop and manage their own local databases outside of PARIS to assign and track inspection activities.

Furthermore, data entered in PARIS may not accurately identify the extent of violations. Inspectors at each airport determine what information should be detailed when documenting the inspections in PARIS, making the inspection data inconsistent and difficult to analyze accurately. We reviewed inspection reports and determined that cargo inspectors documented varying amounts and types of information to support their conclusions, making it difficult to determine the severity of the situation and how many individuals did not meet the requirements. For example, when there were multiple violations, some inspectors would document each individual who did not meet the security threat assessment or the training requirements. Other inspectors would simply note that an entity or authorized representative as a whole did not meet the security threat assessment or training requirements.

Reliance on PARIS is limited because TSA does not provide sufficient guidance, training, and awareness to the inspectors regarding the use of PARIS, the quality and quantity of information entered into PARIS, and the available analysis. After the initial core training, which includes approximately one day of PARIS instructions, TSA does not provide advanced training to help the inspectors learn to use PARIS more efficiently and effectively. One TSA official acknowledged that inspectors do not fully understand how to use PARIS effectively to assist them during the inspection process. Although inspectors have access to find and create many standard reports from

---

PARIS data, some may not have had the necessary training and therefore are unaware that PARIS can generate reports to assist with inspections.

According to TSA officials, the PARIS operational issues are related to the agency's infrastructure problems. These officials indicated that some of the issues could be alleviated if inspectors reduced the number of unnecessary files saved on their computers.

### **Handheld Devices Not Used to Support Inspections**

In 2006, TSA purchased 315 personal digital assistant devices to help automate some of the inspection process. However, the devices were never used as intended. TSA spent at least \$259,000 for the devices to assist inspectors with taking notes and answering prompts from a downloadable version of PARIS. Because use of the equipment would reduce the time inspectors needed to be in the office entering data, inspectors could spend more time in the field performing tests or providing support to ensure security requirements are understood and implemented. TSA also planned for the inspectors to maintain security programs on the handheld devices, making the security regulations readily available during the inspection process.

According to TSA officials, security issues prevented the agency from using the personal digital assistants as planned. After TSA purchased the devices, another federal agency lost a computer containing personal data, elevating concerns regarding the use of all external data and communication devices holding sensitive security information. As a result, TSA instructed the inspectors not to use the personal digital assistants until the agency could implement the required security changes. TSA has decided to purchase other devices and no longer plans to use the personal digital assistant equipment.

---

## **Air Transportation at Risk**

Without an effective inspection process for ensuring compliance with air cargo security requirements, TSA is unable to properly identify and address vulnerabilities, which continue to occur year after year. The aggressive inspection work plan does not focus on high-risk entities, and the agency has challenges with effectively automating the inspection process, both of which hinder TSA's ability to ensure compliance with cargo security requirements. As a result, TSA misses opportunities to strengthen aviation security against the introduction of unauthorized explosive, incendiary, and other destructive substances or items into aircraft cargo, potentially creating a risk to the safety of the traveling public.

### **Recommendations**

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

**Recommendation #1:** Mitigate access control vulnerabilities by:

- a) Requiring more tests for access vulnerabilities and provide corrective actions to the regulated entities;
- b) Placing more focus on entities that are not following the access control requirements; and
- c) Requiring inspectors to spend more time promoting awareness of access control vulnerabilities and their impact on cargo security.

**Recommendation #2:** Improve the security threat assessment process by:

- a) Requiring regulated entities to maintain copies of documents reviewed for authenticating the identity of an applicant;
- b) Revising the application form to include language noting that failure to provide a Social Security

- 
- number may delay or prevent completion of the security threat assessment process; and
- c) Requiring TSA's Office of Transportation Threat Assessment and Credentialing to vet applicants

**Recommendation #3:** Enhance training and testing requirements by providing more specific guidance to regulated entities regarding the training and testing requirements. Additionally, TSA should revise the Regulatory Activities Plan to allow more time for inspectors to review these requirements.

**Recommendation #4:** Revise the Regulatory Activities Plan to allow more time for inspectors to:

- a) Incorporate a risk-based approach that emphasizes the use of historical data and analysis; and
- b) Provide support and education to the regulated entities to ensure that cargo security requirements are understood and implemented.

**Recommendation #5:** Provide better guidance, training, and awareness to all users of the Performance and Results Information System, especially the Transportation Security Inspectors for Cargo. Specifically, develop an action plan for the TSA officials responsible for the Performance and Results Information System to educate the inspectors and ensure optimal use of the available data and analysis. The action plan should also describe:

- a) The quality and quantity of information that should be collected and reported to promote data consistency among field locations;
- b) Types of information and reports available for inspectors to generate from the system as an effective management tool; and
- c) The available analysis in SharePoint to improve risk-based planning reporting capabilities.

---

**Recommendation #6:** Provide Cargo Inspectors with automated tools that will allow them to dedicate more time with the regulated entities. Specifically, establish an action plan, with performance milestones, to address the issues preventing the agency from using the personal digital assistant devices, or similar tools to provide more efficient inspection activities.

## **Management Comments and OIG Analysis**

TSA concurred with five of the recommendations and partially concurred with one of the recommendations in the report. TSA has already begun to formulate plans to implement the recommendations contained in the report. TSA did not provide a complete response on how the agency will address the intent of two recommendations.

### **Management Comments to Recommendation 1:**

TSA Concurs. TSA agrees that access control is a vital part of air cargo security and that aircraft operators, air carriers, and indirect air carriers must prevent unauthorized access to cargo. Inspectors verify compliance with TSA's access control requirements during all comprehensive inspections. Additionally, specific requirements regarding access control for employees or authorized representatives are outlined in the applicable cargo security programs. TSA's Office of Security Operations intends to incorporate additional access control testing protocols in the FY10 Regulatory Activities Plan.

TSA has also worked to address access control vulnerabilities through clear policy requirements for securing air cargo while it is being stored, sorted, screened, and transported. For instance, entities participating in the Certified Cargo Screening Program, have strict facility and transportation access control procedures that include physical security measures such as fences and cameras. TSA is working with outside vendors to explore new transportation security technology, such as testing an electronically serialized locking mechanism as a tamper evident seal. This device is equipped with programmable specific serial numbers with tracking capability, thereby providing enhanced conveyance-level security to Certified Cargo Screening Facility screened cargo.

Cargo inspectors currently spend a significant portion of time providing outreach to Indirect Air Carriers and Certified Cargo Screening Facilities. During the outreach visit, cargo inspectors review all

---

requirements of the applicable Code of Federal Regulations and the Standard Security Program, including ground movement and access control to air cargo. Finally, TSA is conducting Cargo Vulnerability Assessments at the larger airports. TSA is committed to mitigating these vulnerabilities. Vulnerability assessment results are being used to improve policy and operational procedures.

**OIG Analysis:** We recognize TSA's efforts to address the vulnerabilities identified with access control; however, TSA did not respond to the need for more focus on those entities not following access control requirements. This recommendation is resolved and will remain open until TSA provides an action plan or directive that places more emphasis on inspecting those entities not complying with access control requirements. Additionally, TSA indicated that cargo inspectors spend a significant portion of time providing related outreach to Indirect Air Carriers and Certified Cargo Screening Facilities. Based on our review, Indirect Air Carriers demonstrated the need for more time. TSA's response did not discuss how the agency will address the identified need for increased cargo inspectors outreach activities. Once TSA provides the FY10 Regulatory Activities Plan, we will determine whether the additional access control testing protocols will address the need for more testing in this area.

**Management Comments to Recommendation 2:**

TSA concurs. TSA agreed that the concerns with the agency's security threat assessment process should be immediately addressed and partially concurred with the recommendations regarding the Social Security number [REDACTED]. TSA has published an Interim Final Rule on Air Cargo Screening, 74 FR 47672, 47701 (September 16, 2009) that requires that each aircraft operator maintain copies of an applicant's documents used to verify identity and work authorization. TSA also updated the security threat assessment application process and noted that "Failure to furnish this information, including your Social Security number will result in delays in processing your application and may prevent completion of your security threat assessment."

TSA will evaluate the process to require [REDACTED] [REDACTED] for air cargo workers, the costs of necessary system and database changes to capture biometrics, and the number of new-hire adjudicators to execute evaluations. Additionally, the agency will review the required increase in fees to cover the vetting process.

---

**OIG Analysis:** TSA's response indicates that the agency shares our concerns regarding the security threat assessment process. This recommendation is resolved, but will remain open until the agency updates the OIG on the condition of its proposed corrective actions. TSA should provide details regarding what supporting documentation will be maintained for the security threat assessment applicants, and what actions will be taken based on results of the evaluations focused of the process for ensuring

### **Management Comments to Recommendation 3**

**TSA Concur.** TSA concurs that training and testing of air cargo security requirements are important and will continue to ensure proper regulatory oversight. TSA specifies training and testing requirements in its security programs, which stipulate the minimum training content, training frequency, training log requirements, testing frequency, and passing scores for tests.

TSA is beginning to standardize training and testing, which it plans to require for all regulated parties. Cargo inspectors verify compliance with TSA training and testing requirements during inspections. Non-compliant entities are counseled on how to obtain the proper security training and testing. TSA cargo inspectors verify compliance with training and testing requirements as part of all comprehensive inspections.

**OIG Analysis:** Based on TSA's response, this recommendation is resolved, but will remain open until we have obtained and reviewed the FY10 Regulatory Activities Plan and the details on the standardized training and testing. TSA should provide supporting documentation to show how the agency will ensure all regulated entities receive the new training and pass the tests. TSA should also specify how the cargo inspectors will verify that the regulated entities ensure their authorized representatives are properly trained and tested.

### **Management Comments to Recommendation 4**

**TSA Concur.** TSA is currently developing the FY10 Regulatory Activities Plan to include a risk-based approach to inform inspections. The new approach will provide a risk score per regulated entity per location, which means that regulatory personnel will be able to access risk scores specific to their airport. Inspections will be driven based on each entity's score, local and national intelligence, and responses to significant national events or identification of systematic vulnerabilities.

---

**OIG Analysis:** This recommendation is resolved, but will remain open until we have obtained and reviewed the FY 2010 Regulatory Activities Plan to ensure the risk-based approach is clearly presented in the guidance. TSA should also provide details regarding the agency's improved efforts to work closely with aviation industry stakeholders to provide support and education.

**Management Comments to Recommendation 5**

**TSA Concur.** TSA's Air Cargo Compliance Division has continued to perform quality control review audits of PARIS entries submitted by field elements. The inspection quality control reviews focus on compliance with the National Inspection Manual and Regulatory Activities Plan requirements. TSA headquarters shares this information with Assistant Federal Security Directors for Inspections upon request and allows them to take appropriate actions when necessary to ensure the PARIS entries submitted by their staff are in compliance with the National Inspection Manual and Regulatory Activities Plan requirements.

TSA provides cargo inspectors with PARIS training and guidance materials to more efficiently use PARIS and generate reports on data contained in PARIS. Training is also provided on the conversion of data extracted from PARIS into Excel spreadsheet pivot tables. This training provides cargo inspectors with the ability to generate more useful reports on inspection, investigation outreach, and incident data, and analyze and organize the reports in a fashion tailored to their needs. The training is provided through the cargo inspector's initial, on the job, and recurrent training. Also, the PARIS program office has developed a comprehensive series of user guides and on-line demos.

TSA provides a PARIS application Help Desk Phone Line, an information technology single point of contact, and support from PARIS staff members. The agency also relies on its contractor-based support system that TSA uses for its enterprise information technology applications. Inspectors can also use the PARIS Blog and SharePoint for communications regarding air cargo related risks.

**OIG Analysis:** TSA's response identified the agency's efforts to provide training on the use of PARIS; however, it does not address the underlying concern that cargo inspectors may not fully understand and use the available resources to understand PARIS capabilities. While TSA provides support, training, and guidance to more efficiently use

---

PARIS, more needs to be done to ensure its use is maximized. This recommendation is resolved, but will remain open until TSA can provide evidence that field cargo inspectors are knowledgeable on generating useful PARIS reports. TSA should provide an action plan and supporting documentation to demonstrate how local airports are effectively utilizing PARIS and generating useful reports to assist with inspection activities.

**Management Comments to Recommendation 6**

**TSA Concurrs in part.** TSA is moving forward with a plan to provide more modern and advanced tools to assist the inspectors and their activities. TSA no longer plans to use the personal digital assistant equipment. Instead, TSA has procured other automated devices that will be distributed to the cargo inspectors by the conclusion of FY 2009. For example, TSA has acquired blackberries with a camera feature; document hand scanners; test phones for special emphasis inspections and small package testing; and laptops for all Cargo Inspectors. In addition to securing new productivity tools, TSA has been working to streamline the record-keeping requirements associated with documenting inspections.

**OIG Analysis:** This recommendation is resolved, but will remain open until TSA provides evidence to show the agency has completed the distribution of the procured tools listed in the agency's response. Specifically, TSA should provide the distribution schedule for all items and evidence that these tools are being fully utilized to avoid the experienced waste identified with the personal digital assistant equipment acquisitions.

## **Appendix A**

### **Purpose, Scope, and Methodology**

---

The objective of our audit was to determine the effectiveness of TSA's efforts to ensure the security of air cargo during ground transportation and handling before it is loaded onto planes.

We obtained and reviewed applicable federal laws and regulations, TSA's standard security programs, security directives, the 2008 and 2009 Regulatory Activities Plans, the National Inspection Manual, the Air Cargo Strategic Plan, and other related documents.

We interviewed TSA personnel from the Offices of Transportation Threat Assessment and Credentialing, Office of Security Operations, Office of Chief Counsel, and the Transportation Sector Network Management Division.

During our survey work and audit fieldwork, we visited five airports: Chicago O'Hare International, Washington-Dulles International, Minneapolis St. Paul International, Miami International, and Los Angeles International. During our site visits, we interviewed and accompanied TSA cargo inspectors to observe operations and interview personnel at aircraft operators, all-cargo operators, and indirect air carrier facilities.

At two of the airports, we judgmentally selected air carriers and obtained a nonstatistical sample of airway bills to trace back to indirect air carriers to determine whether the drivers on the airway bill documentation had met TSA's security program requirements, including the security threat assessment and security training. This test included a review of security threat assessment and training requirements for 104 truck drivers from 36 indirect air carriers.

We conducted a review and analysis of the following 11 airports that transported a large amount of freight:

- Los Angeles International
- John F. Kennedy International
- Chicago O'Hare International
- Miami International
- Hartsfield-Jackson Atlanta International
- San Francisco International

## Appendix A

### Purpose, Scope, and Methodology

---

- Washington-Dulles International
- Newark-Liberty International
- Houston Intercontinental
- Honolulu International
- Minneapolis St. Paul International

We interviewed personnel responsible for the PARIS database from the Office of Security Operations Compliance Inspection and Enforcement Team. We received a demonstration of the system's capabilities and requested specific searches and reports to determine what information is available to TSA inspectors and officials. We obtained TSA summary reports documenting the total number and type of inspections each airport performed on cargo at each location from January through September 2008. We also obtained several reports summarizing the numbers and types of violations that inspectors disclosed during their inspections. We judgmentally selected and analyzed inspection reports to determine the types of violations identified by the inspectors, actions taken to resolve the issues, and the level of detail that the inspectors provided in the reports.

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 January and April 2009 under the authority of the *Inspector General Act of 1978*, as amended.

## Appendix B Management Comments to the Draft Report

---

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

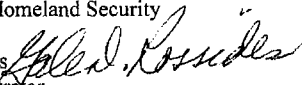
OCT 05 2009



Transportation  
Security  
Administration

### INFORMATION

MEMORANDUM FOR: Richard Skinner  
Inspector General  
Department of Homeland Security

FROM: Gale D. Rossides   
Acting Administrator

SUBJECT: Draft Report: "Security of Air Cargo during Ground  
Transportation," July 2009

#### Purpose

This memorandum constitutes the Transportation Security Administration's (TSA) formal agency response to the Department of Homeland Security (DHS) Office of Inspector General (OIG) draft report, "Security of Air Cargo during Ground Transportation" dated July 2009.

#### Background

The Office of the Inspector General conducted this investigation to evaluate the effectiveness of TSA's efforts to secure cargo while it is handled or transported on the ground, prior to being shipped on passenger aircraft. OIG found that TSA's inspection process has focused on quantity rather than outcomes and ensuring corrective actions. Automated tools to assist inspectors in analyzing results and focusing their oversight efforts on high-risk areas in air cargo security were not adequate. OIG makes six recommendations to strengthen the security of air cargo ground transportation.

#### Discussion

The *Implementing the Recommendations of the 9/11 Commission Act of 2007* requires TSA to establish a system for industry to screen 100 percent of cargo transported on passenger aircraft in the United States to provide a level of security that is commensurate with the level of security for the screening of passenger baggage. The legislation also set an interim milestone of 50 percent screening to be reached by February 2009. By August 2010, cargo not screened in accordance with TSA-approved processes and procedures cannot be uplifted to a passenger aircraft in the United States.

This is an extensive requirement and, TSA understands there is simply not sufficient capacity or space in airports to meet its demands without carrier delays, cargo logjams, and increased transit

## Appendix B

### Management Comments to the Draft Report

---

2

times. Therefore, TSA has established a multi-dimensional strategy to reconcile the requirements of the mandate, the security needs of passengers, and the needs of a U.S. economy reliant upon the air cargo industry.

In addition to TSA's existing security regime, we have established three programs to assist in meeting the 100 percent screening mandate and have made excellent progress:

- 100 Percent Narrow-Body Screening – 100 percent of cargo uplifted on narrow-body passenger aircraft has been screened since October 2008. This program accounts for 96 percent of passenger flights originating in the US and its territories, and covers approximately 25 percent of the cargo uplifted in the US.
- The Certified Cargo Screening Program (CCSP) – A voluntary program designed to enable certain vetted, validated, and certified facilities to screen cargo prior to delivering the cargo to the air carrier. To date, the majority of air cargo screening is done by air carriers through CCSP.
  - TSA has certified 477 cargo screening facilities through the program.
  - An interim final rule to accelerate the deployment of the program was published in the *Federal Register* on September 16, 2009, and will take effect on November 16, 2009. During initial deployment of CCSP, the onsite facility assessment has been performed by a TSA Field Team staff. TSA expects that during full rollout, assessments will be performed by a TSA-approved validation firm.
- Indirect Air Carrier (IAC) Screening Technology Pilot – an initiative established to test screening technology in a live environment.
  - Participants in this program are working directly with TSA to provide information and data on cargo, commodity-types, and a certain cargo screening technology. Information collected from this pilot will impact future TSA decisions on acceptable screening technologies.
  - There are 91 participating locations receiving approximately \$40.6 million in technology assistance.
- TSA Explosives Detection Canine Programs – TSA certified explosives detection canine teams are available to screen cargo throughout the network.
  - 465 law enforcement partner canine teams devote a part of their time to screening cargo; 6 additional teams will graduate in fiscal year (FY) 2009
  - 84 TSA proprietary canine teams are fully dedicated to screening cargo. 36 more teams are authorized and planned for deployment in FY 2010, 19 of which have been hired and are currently in training.

TSA agrees that access control is a vital part of air cargo security. In addition to our operational oversight, we will continue to work to address access control vulnerabilities through clear policy requirements for securing air cargo while it is being stored, sorted, screened, and transported. We are in agreement that the concerns that have been identified with the agency's security threat assessment process should be addressed, and we are providing more guidance and tools to standardize training. TSA's Office of Security Operations (OSO) FY 2010 Regulatory Activities Plan (RAP) incorporates a risk-based approach to inspections. In FY 2009, OSO Air Cargo Compliance has continued to perform Quality Control (QC) and review audits of Performance and Results Information System (PARIS) entries submitted by field elements. Lastly, TSA will

## Appendix B

### Management Comments to the Draft Report

---

3

provide cargo inspectors with automated tools that will allow them to dedicate more time with regulated entities.

Overall, we believe that the recommendations contained in the report will provide additional benefit to TSA. TSA has already begun to formulate plans to implement the recommendations contained in the report. Our specific response to each recommendation follows.

**Recommendation #1: Mitigate access control vulnerabilities by:**

- a) **Requiring more tests for access vulnerabilities and provide corrective actions to the regulated entities;**
- b) **Placing more focus on entities that are not following the access control requirements; and**
- c) **Requiring inspectors to spend more time promoting awareness of access control vulnerabilities and their impact on cargo security.**

**TSA Concurs:** TSA agrees that access control is a vital part of our layered approach to air cargo security.

- a) TSA's Office of Security Operations (OSO) intends to incorporate additional access control testing protocols in the FY 2010 Regulatory Activities Plan (RAP). The RAP is the basis for a Transportation Security Inspectors (TSIs) annual work plan. These additional tests will augment the current system in place. OSO will continue to inspect drivers on their training and knowledge of their security functions.

Inspectors verify compliance with TSA's access control requirements during all comprehensive inspections. In addition, TSA performed a special emphasis inspection (SEI) during FY 2009 Q2 specifically concentrated on access control. The objective of this SEI was to determine, through realistic testing, if foreign air carriers, aircraft operators, and indirect air carriers (IACs) properly control access to cargo as required under transportation security regulations in 49 Code of Federal Regulations (CFR) and appropriate cargo security programs. Aircraft operators, foreign air carriers and IACs must prevent unauthorized access to cargo in accordance with 49 CFR Sections 1544.205(c), 1544.228, 1546.205(c), 1546.213, 1548.5, and 1548.15. Additionally, specific requirements regarding access control for employees or authorized representatives are outlined in the applicable cargo security programs. The SEI protocol stipulated that all instances of non-compliance receive a formal investigation. Cases could be resolved with either administrative or civil penalty action. Counseling alone could not be used as a means to close any violations discovered. Finally, SEI results are being used to identify trends in vulnerabilities, assist in identifying corrective measures (e.g., policy or operational), and formulate additional access control testing protocols.

## Appendix B

### Management Comments to the Draft Report

---

4

- b) TSA is working with our partners to identify new access control mechanisms. Through partnership with outside vendors we are exploring new conveyance security technology. For instance, TSA has authorized a pilot at Detroit Metropolitan Wayne County Airport called M-lock. The M-lock is an electronically serialized locking mechanism which TSA is testing as a tamper evident seal. This device is equipped with programmable specific serial numbers which are displayed on an LED screen with GPS tracking capability, thereby providing enhanced conveyance-level security to Certified Cargo Screening Facility (CCSF)-screened cargo. Currently, TSA is conducting Cargo Vulnerability Assessments at all Cat X and Cat I airports. TSA is committed to mitigating these vulnerabilities. Vulnerability assessment results are being used to improve policy and operational procedures. In addition to our operational oversight, TSA has worked to address access control vulnerabilities through clear policy requirements for securing air cargo while it is being stored, sorted, screened, and transported. Entities participating in the Certified Cargo Screening Program (CCSP), for instance, have strict facility and conveyance access control procedures that include physical security measures (e.g., fences, cameras), employee identification media, chain of custody technology applied to the screened cargo, and secured conveyances (e.g., locked, sealed, or vehicles under escort).
- c) As of the date of this report, TSIs have conducted over 2,060 outreach efforts directly related to air cargo security. TSIs currently spend a significant portion of time providing outreach to Indirect Air Carriers and CCSFs both prior to their becoming certified and after. Prior to an IAC becoming approved, they must submit to a TSI Outreach visit. During this visit the TSI reviews all requirements of the applicable Code of Federal Regulations and the Standard Security Program itself. This includes ground movement and access control to air cargo. TSIs review the facility and trucks to determine if in their current state, they would adequately be able to meet requirements. If not, the TSI will work with the entity to achieve the appropriate level of ground movement and access control security prior to approval.

In regard to CCSFs, TSA also has a lengthy application process that requires constant interaction and outreach provided by Principal Cargo Security Analysts (PCSAs). These TSA personnel work with an entity to help them achieve the required security level through outreach and education. A CCSF must be "certified" by a PCSA prior to entrance into the program

**Recommendation #2: Improve the security threat assessment process by:**

- a) **Requiring regulated entities to maintain copies of documents reviewed for authenticating the identity of an applicant;**

## Appendix B

### Management Comments to the Draft Report

---

5

- b) **Revising the application form to include language noting that failure to provide a social security number may delay or prevent completion of the security threat assessment process and;**
- c) **Requiring TSA's Office of Transportation Threat Assessment and Credentialing to vet applicants**

**TSA Concur:** TSA agrees that the concerns that have been identified with the agency's security threat assessment process should be addressed and partially concurs with the recommendations on social security number (SSN)

- a) TSA concurs. TSA has just published an Interim Final Rule on Air Cargo Screening, 74 FR 47672, 47701 (September 16, 2009) (Air Cargo Screening IFR) that requires that each aircraft operator maintain copies of the applicant's documents used to verify identity and work authorization.
- b) Currently, language in the Privacy Act Notice found in 49 CFR §1540.203(b)(2)(viii) regarding security threat assessments provides that: "Failure to furnish your SSN may result in delays in processing your application, but will not prevent completion of your Security Threat Assessment." However, TSA's recently published Air Cargo Screening IFR contains the language that the IG recommends: "Failure to furnish this information, including your Social Security Number (SSN) will result in delays in processing your application and may prevent completion of your security threat assessment." 74 FR at 47683.
- c) TSA recognizes the importance of utilizing the best method possible to capture and evaluate the history of those who will have ready access to our nation's air cargo transportation system. TSA will evaluate the process to require  
for air cargo populations, the costs of necessary system/database changes that would capture biometrics, and the number of new-hire adjudicators to execute the evaluation process. Additionally, we will review the required increase of fees to cover the vetting process.

**Recommendation #3: Enhance training and testing requirements by providing more specific guidance to regulated entities regarding the training and testing requirements. Additionally, TSA should revise the Regulatory Activities Plan to allow more time for inspectors to review these requirements.**

**TSA Concur:** TSA specifies training and testing requirements in the aircraft operator, IAC, and CCSP security programs. The security programs clearly stipulate the minimum training content, frequency of training, training log requirements, testing frequency, and passing scores for tests. In addition, TSA provides the IACs with TSA-approved training materials and tests for their Security Coordinators, direct employees, and authorized representatives. We are currently developing comparable materials for the aircraft operators and CCSFs. In addition, TSA is beginning the process of developing standardized training and testing, which it plans to require for all regulated parties.

## Appendix B

### Management Comments to the Draft Report

---

6

TSA verify compliance with TSA training and testing requirements during inspections. Non-compliant entities are counseled on how to obtain the proper security training and testing. In addition, TSIs routinely conduct outreach to the regulated air cargo community.

TSA will be revising the FY 2010 RAP. TSA concurs that training and testing of air cargo security requirements are important and will continue to ensure proper regulatory oversight as such. TSA cargo inspectors verify compliance with training and testing requirements as part of all comprehensive air carrier, IAC, and CCSF inspections.

**Recommendation #4: Revise the Regulatory Activities Plan to allow more time for inspectors to:**

- a) **Incorporate a risk-based approach that emphasizes the use of historical data and analysis.**
- b) **Provide support and education to the regulated entities to ensure that cargo security requirements are understood and implemented.**

**TSA Concurs:** TSA's FY 2010 RAP addresses these concerns.

- a) TSA's FY 2010 RAP incorporates a risk-based approach to inform inspections. We have developed a risk score for every entity regulated under a TSA air cargo security program. Our approach provides a risk score per regulated entity per location, which means that Regulatory personnel will be able to access risk scores specific to their airport. Risk scores are updated quarterly. Inspections will be driven based on the entities score: red, yellow, or green indicators. Inspections will also be driven by local and national intelligence as well as responses to significant national events or identification of systematic vulnerabilities; and
- b) TSA will continue to work closely with aviation industry stakeholders to provide support and education.

**Recommendation #5: Provide better guidance, training and awareness to all users of the Performance and Results Information System, especially the Transportation Security Inspectors for Cargo. Specifically, develop an action plan for the TSA officials responsible for the Performance and Results Information System to educate the inspectors and ensure optimal use of the available data and analysis. The action plan should also describe:**

- a) **The quality and quantity of information that should be collected and reported to promote data consistency among field locations;**
- b) **Types of information and reports available for inspectors to generate from the system as an effective management tool; and**
- c) **The available analysis in Share Point to improve risk-based planning reporting capabilities.**

## Appendix B

### Management Comments to the Draft Report

---

7

#### TSA Concur:

- a) In FY 2009, TSA's OSO Air Cargo Compliance has continued to perform Quality Control (QC) review audits of PARIS entries submitted by field elements. Each quarter, OSO Cargo Compliance selects PARIS inspection reports for airports and Cargo TSIs in each area to review for QC. The inspection QC reviews focus on compliance with the National Inspection Manual (NIM) and RAP requirements. The goal is to review at least one report from each Cargo TSI at each airport by the end of the fiscal year. Headquarters (HQ) shares this information with Assistant Federal Security Director's for Inspections upon request and allows them to take appropriate actions when necessary to ensure the PARIS entries submitted by their staff are in compliance with the NIM and RAP requirements.
  
- b) In addition, TSA's OSO Compliance Programs provide PARIS training and guidance materials. This training involves tips on how to more efficiently use PARIS and on generating reports on data contained in PARIS. Training is also provided on the conversion of data extracted from PARIS into Excel Spreadsheet "Pivot Tables." This training provides TSIs with the ability to generate more useful reports on inspection, investigation outreach and incident data, and analyze and organize the reports in a fashion tailored to their needs. This is primarily facilitated through three efforts. First, newly hired TSIs receive PARIS training during the "Transportation Security Inspector Basic Training Program," a comprehensive four week training regime at TSA's Security Enforcement Training Academy. This training is conducted via presentation and hands on exercises. This training is continued during the new TSIs official on the job training (OJT). Second, experienced TSIs receive a refresher during recurrent training. Recurrent training is held at least once a quarter at various airports throughout the country with the goal of all experienced inspectors attending at least one session a year. Third, the PARIS program office has developed a comprehensive series of user guides and on-line demos.  
  
Furthermore, in the interest of facilitating swift and effective communications between the PARIS User Community and the PARIS Support staff at HQ, TSA OSO, Inspection Enforcement and Analysis Branch established a PARIS application Help Desk Phone Line in the TSA Phone Network. Field personnel can call HQ personnel and speak to a PARIS support staff member. This additional communication channel is intended to offer an additional convenient means for PARIS users to talk to one of the experts who supports the PARIS program. It does not replace the agency's information technology (IT) single point of contact (i.e., SPOC) and the contractor-based support system that TSA uses for its enterprise IT applications. Rather, it is an opportunity for us to bring increased support to the PARIS user community as it relates to the PARIS application itself. The SPOC remains the first contact for any functional anomalies. Field Inspectors can also reach the help desk support through the PARIS Blog.
  
- c) The Office of Compliance publishes periodic reports into Sharepoint, an internal electronic tracking system. This system is available to all inspectors who perform oversight as well as staff who analyze inspection reports.

## Appendix B

### Management Comments to the Draft Report

---

8

**Recommendation #6: Provide Cargo Inspectors with automated tools that will allow them to dedicate more time with the regulated entities. Specifically, establish an action plan, with performance milestones, to address the issues preventing the agency from using the personal digital assistant devices to provide more efficient inspection activities.**

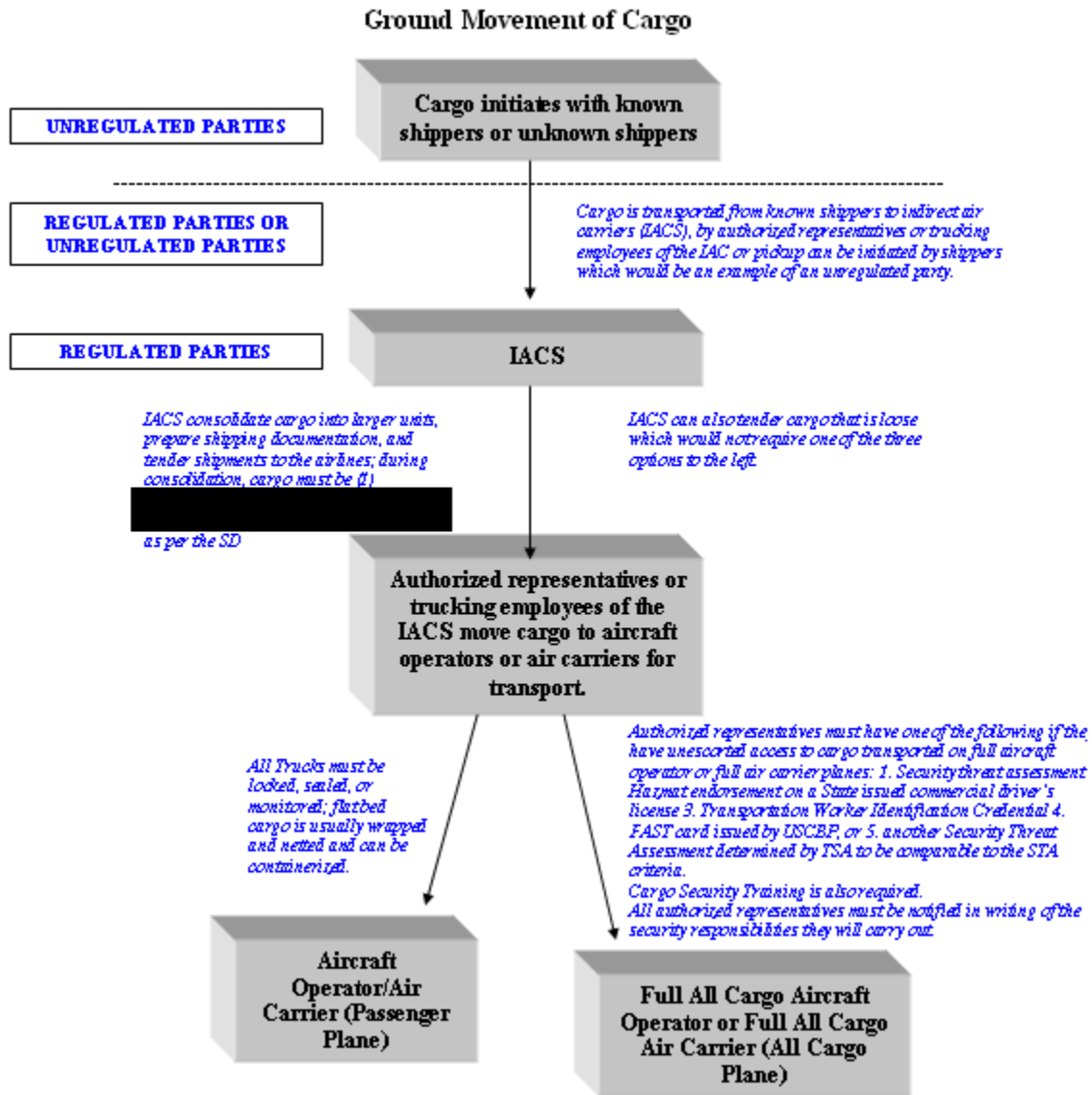
**TSA Concurrs in Part:** TSA believes that the personal digital assistant devices (PDAs) are antiquated technology and are not efficient. We are moving forward with a plan to provide more modern and advanced tools to our regulatory workforce to improve productivity. These include, but are not limited to:

- Blackberries, with camera feature, for all inspectors.
- Document hand scanners. This device allows TSIs to make copies of records. We have secured one per airport.
- Test phones for special emphasis inspections and small package testing. One test phone per airport with assignment of a new number every 6 months.
- Laptops for all cargo inspectors.
- Dedicated cargo vehicles. We improved the ratio of one vehicle for every two inspectors at the airport.
- One GPS unit per cargo vehicle.
- Air cards for communal use among Regulatory personnel.

These tools have already been procured and will be dispersed to the TSIs by the conclusion of FY 2009.

In addition to securing new productivity tools, TSA's OSO has been working to streamline the record keeping requirements associated with documenting inspections. For instance we revised the PARIS prompts for the passenger and all cargo air carrier and IAC inspection types. Specifically we reduced the number of prompts by 40-50 percent while still capturing all the requirements. This reduces the amount of entry time per PARIS inspection record, and allows the Inspector more discretion on the level of detail to input.

**Appendix C**  
**Process for Ground Transportation of Air Cargo**



**Appendix D**  
**Security Threat Assessment Requirements**

**Who Needs an STA under the IACSSP?**

People who meet one of the following requirements **NEED** an STA:

1. Screen Air Cargo **OR**
2. Are an IAC proprietor, IACSC or alternate IACSC, general partner, director, officer, or owner **OR**
3. Meet A **OR** B

<b>A</b>	<b>B</b>
<p style="text-align: center;"><b>Have <u>unescorted</u> access to air cargo:</b></p> <ul style="list-style-type: none"> <li>• At a facility* until the cargo enters a SIDA (or secure area) or is transferred to another IAC, a full passenger or full all cargo program holder or</li> <li>• That is transported from the facility* to another IAC, a full passenger or full all-cargo program holder</li> </ul> <p style="text-align: center;"><b>AND</b></p> <p><b>Have access to information that the cargo will travel on a <u>PASSENGER AIRCRAFT</u></b></p>	<p style="text-align: center;"><b>Have <u>unescorted</u> access to air cargo:</b></p> <ul style="list-style-type: none"> <li>• At a facility* until the cargo enters a SIDA (or secure area) or is transferred to another IAC, a full passenger or full all cargo program holder or</li> <li>• That is transported from the facility* to another IAC, a full passenger or full all-cargo program holder</li> <li>• That is accepted from a shipper and ground transported to another IAC, full passenger or full all-cargo program holder</li> </ul> <p style="text-align: center;"><b>AND</b></p> <p><b>Perform one of the following duties for air cargo transported on <u>PASSENGER AIRCRAFT</u> or <u>ALL-CARGO AIRCRAFT</u>:</b></p> <ul style="list-style-type: none"> <li>• Lock, or seal, or monitor air cargo or</li> <li>• Dispatch vehicles to transport air cargo to an on-airport facility* or</li> <li>• Transport air cargo to an on-airport facility* or</li> <li>• Monitor air cargo at a facility*</li> </ul>

\*Facility = refers to an area outside of a SIDA where air cargo is stored, sorted, held, built-up, consolidated, containerized or screened

**The following are accepted instead of an air cargo STA:**

- CHRC in accordance with 49 CFR 1542.209, 1544.229 and 1544.230
- Free and Secure Trade (FAST) card
- Valid Commercial Drivers License (CDL) with HAZMAT Endorsement (HME) issued within the 50 states and the District of Columbia
- Transportation Worker Identification Card (TWIC)
- Any other background check that may be approved by TSA as comparable to an STA

**Appendix E**  
**Major Contributors to This Report**

---

Patrick O'Malley, Director  
Cecilia Barela, Desk Officer  
Sandra Ward Greer, Project Lead  
Andrew Herman, Auditor  
Kathleen Hyland, Auditor  
Amy Nase, Auditor  
Raul Quintero, Program Analyst  
James Bess, Referencer

**Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff for Operations  
Chief of Staff for Policy  
General Counsel  
Executive Secretary  
Director, GAO/OIG Liaison Office  
Assistant Secretary for Office of Policy  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs  
DHS Component Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees, as appropriate

### **Additional Information and Copies**

To obtain additional copies of this report, 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](http://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;
- E-mail us at [DHSOIGHOTLINE@dhs.gov](mailto: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.



#### ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at [www.dhs.gov/oig](http://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](mailto: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.